VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra aplikované matematiky

Kritéria dělitelnosti

Divisibility Criterions

2014

Veronika Balcárková

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra aplikované matematiky

Zadání bakalářské práce

Student: **Veronika Balcárková**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 1103R031 Výpočetní matematika

Téma: Kritéria dělitelnosti
Divisibility criterions

Zásady pro vypracování:

Jedná se o jeden z mnoha výsledků teorie čísel. Pomocí kritérií dělitelnosti můžeme rozhodnout, zda je dané číslo (zapsané ciframi určité číselné soustavy) dělitelné daným číslem. Je proto výhodné použít tato kritéria jako první síto při identifikaci prvočísel.

V bakalářské práci by mělo být obsaženo:
1. Matematické odvození kritérií dělitelnosti prvočísly do stanovené velikosti a to v různých číselných soustavách.
2. Možnosti použití jako prvního síta při hledání "velkých" prvočísel.
3. SW umožňující aplikaci kritérií dělitelnosti a poskytující odhad počtu prvočísel v daném intervalu.

Seznam doporučené odborné literatury:

Kolibiar, M., Legéň, A., Šalát, T., Znám, Š.:*Algebra a príbuzné disciplíny*, Bratislava, Alfa, 1992.

Šlát,T.: *Algebra a teoretická aritmetika 2*, Bratislava, Alfa, 1986.

Znám, Š.: *Teória čísel*, Bratislava, Alfa, 1986.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **RNDr. Pavel Jahoda, Ph.D.**

Datum zadání: 01.09.2013
Datum odevzdání: 07.05.2014

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA Fakulta elektrotechniky a informatiky OSTRAVA

doc. RNDr. Jiří Bouchala, Ph.D.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlašuji, že jsem tuto bakalářskou práci vypracovala samostatně. Uvedla jsem všechny literární prameny a publikace, ze kterých jsem čerpala.

V Ostravě 7. května 2014

Balcárková

.....

Ráda bych na tomto místě poděkovala mému vedoucímu bakalářské práce RNDr. Pavlu Jahodovi, Ph.D. za veškerou pomoc a poskytnutí materiálů při psání této bakalářské práce. A zároveň bych chtěla poděkovat své rodině a nejbližším za obrovskou psychickou podporu během studií.

Abstrakt

Tato bakalářská práce se zabývá jednou z oblastí teorie čísel. První část této práce se zabývá základními vlastnostmi dělitelnosti na okruhu celých čísel. Druhá část práce se věnuje relaci kongruence. Třetí část je nejrozsáhlejší a zabývá se jednotlivými kritérii dělitelnosti v desítkové a binární číselné soustavě. Poslední část je věnována matematickým výpočtům v programu MATLAB, kde jsou aplikována kritéria dělitelnosti obsažená v této bakalářské práci. Vytvořený program poskytuje hrubý horní odhad počtu prvočísel v různě velkých intervalech a seznam čísel, která i po použití vybraných kritérií dělitelnosti zůstávají v podezření, že jde o prvočísla.

Klíčová slova: teorie čísel, kritéria dělitelnosti, kongruence, desítková soustava, binární soustava, MATLAB, prvočíslo

Abstract

This Bachelor Thesis deals with one of the section of Number Theory. The first part of this Bachelor Thesis deals with basic properties of divisibility on the circuit of integers. The second part dedicates a congruence relation. The third part is the largest part and deals with divisibility criterions in decimal and binary system. The last part is dedicated to mathematical calculations in MATLAB, where are applicated the divisibility criterions, which are conteined in this Bachelor Thesis. The program provides an rough upper estimate of the prime numbers in different sized intervals and a list of numbers that even after applying the divisibility criterions remain under suspicion that these are prime numbers.

Keywords: Number Theory, Divisibility Criterions, congruence, decimal system, binary system, MATLAB, prime number

Seznam použitých zkratek a symbolů

$\mathbb{N}$	–	množina přirozených čísel
$\mathbb{Z}$	–	množina celých čísel
$b \vert a$	–	číslo b dělí číslo a
$gcd(a, b)$	–	největší společný dělitel
$n(a, b)$	–	nejmenší společný násobek
$A \times B$	–	kartézský součin množiny A a B
$R \subseteq A \times A$	–	binární relace na množině A
$a \wedge b$	–	a a zároveň b
$a \vee b$	–	a nebo b
$a \Rightarrow b$	–	a implikuje b
$\equiv$	–	relace kongruence
$a \equiv b (\mathrm{mod} m)$	–	a je kongruentní s b modulo m
$\sum_{i=0}^{k}$	–	suma jdoucí od 0 do k

Obsah

Seznam výpisů zdrojového kódu

Seznam obrázků

1 Úvod

Teorie čísel je jedna z nejzákladnějších oblastí matematiky, která zkoumá vlastnosti jednotlivých čísel. Zabývá se většinou celými čísly, ale není to pravidlem. Tato bakalářská práce je zaměřena na kritéria dělitelnosti v oboru celých čísel a je rozdělena do 4 částí.

V Kapitole 2 se seznámíme s dělitelností na množině celých čísel, co je to největší společný dělitel, nejmenší společný násobek, nebo jak funguje Euklidův algoritmus a k čemu nám slouží. Dostaneme se postupně až ke kanonickému rozkladu čísel a k základní větě aritmetiky.

Kapitola 3 pojednává o kongruencích na množině celých čísel. Povíme si, co to jsou relace, jaké druhy relací známe a čím jsou typické. Budeme se zabývat dělitelností čísel se zbytkem, konkrétně o kongruenci modulo m. Velmi důležitou částí třetí kapitoly je Malá Fermatova věta. Tuto větu využijeme při určování některých kritérií dělitelnosti.

Dříve zmíněné kapitoly jsme potřebovali k tomu, abychom se dostali k hlavnímu cíli této práce - odvození vybraných kritérií dělitelnosti. Kapitola 4 je tedy věnována některým kriteriím dělitelnosti. Jsou zde vypsány a dokázány kritéria od čísla 2 po číslo 12 v desítkové a binární soustavě. Tyto kritéria jsou dokazována pomocí kongruencí, o kterých si povídáme ve třetí kapitole. U každé dělitelnosti některého z čísel je uveden důkaz i příklad, ve kterém je postup výpočtu. Na závěr kapitoly je odvozen obecný postup, jak určit kritérium dělitelnosti prvočíslem.

Poslední kapitola je věnována ukázce matematických výpočtů v programu MATLAB. Jsou zde aplikovány kritéria prvočísel obsažených v předchozí kapitole, tj. dělitelnost dvěma, třemi, pěti, sedmi a jedenácti, která pomáhají k výpočtům. Cílem bylo zaměřit se na velké množství čísel a aplikací těchto kritérií shora odhadnout, kolik prvočísel se nachází v daných, různě velkých intervalech. V programu je také zahrnuta funkce měření času, jak dlouho trvalo odhadnout počet prvočísel z intervalu. Z vygenerovaných grafů můžeme vidět, jak vzrůstá čas se zvětšujícím se intervalem, ale ne vždy to trvá stejně, povíme si i o faktorech, které ovlivňují celkový čas výpočtu.

Všechny grafy a pomocné výpočty, které jsou obsaženy v této bakalářské práci, byly vytvořeny pomocí skriptovacího programovacího jazyku čtvrté generace v programu MATLAB od společnosti MathWorks.

2 Dělitelnost na množině celých čísel

2.1 Základní vlastnosti dělitelnosti

Již na základní škole jsme se setkali s pojmem dělitelnost, který je jedním ze základních v elementární teorii čísel. Vyskytují se zde pojmy jako *násobek* a *dělitel*.

Definice 2.1 *Mějme nějakou dvojici čísel $a, b \in \mathbb{Z}$. Pak číslo a je dělitelné číslem b, právě tehdy když existuje takové číslo $k \in \mathbb{Z}$, že platí*

$$a = k \cdot b.$$

Píšeme, že $b|a$.

Příklad 2.1
Nalezněte nějaké dělitele čísla 18.

$18 = 18 \cdot 1$
$18 = 2 \cdot 9$
$18 = 3 \cdot 6$

Můžeme říci, že dělitele čísla 18 jsou například čísla 1, 6 a 9.

Lemma 2.1 *Pro každé číslo $a \in \mathbb{Z}$ platí:*

(i) $a|0$

(ii) $1|a$

(iii) $a|a$

Důkaz.

(i) Pro každé $a \in \mathbb{Z}$ platí, že $0 = 0 \cdot a$. Protože $0 \in \mathbb{Z}$, můžeme podle Definice 2.1 psát $a|0$.

(ii) Pro každé $a \in \mathbb{Z}$ platí, že $a = a \cdot 1$. Protože $a \in \mathbb{Z}$, můžeme podle Definice 2.1 psát $1|a$.

(iii) Pro každé $a \in \mathbb{Z}$ platí, že $a = 1 \cdot a$. Protože $1 \in \mathbb{Z}$, můžeme podle Definice 2.1 psát $a|a$.

■

Předchozí Lemma 2.1 říká, že nula je dělitelná každým číslem $a \in \mathbb{Z}$. Dále, že libovolné číslo $a \in \mathbb{Z}$ je dělitelné sebou samým a jakékoliv číslo $a \in \mathbb{Z}$ je dělitelné jedničkou.

Navíc musíme říci, že nula není dělitelem žádného čísla $a \in \mathbb{Z}$, kde $a \neq 0$. Ukážeme si to v následujícím příkladě.

Příklad 2.2
Nalezněte všechna celá čísla dělitelná číslem 0.

Do rovnosti $a = k \cdot b$ z Definice 2.1 dosadíme za b nulu a dostaneme $a = k \cdot 0$. Každé číslo, které vynásobíme nulou, bude vždycky 0. To znamená, že také $a = 0$. Z toho vyplývá, že pouze číslo 0 je dělitelné nulou.

Lemma 2.2 [1] *Pro dělitelnost na množině $\mathbb{Z}$ platí:*

1. *Pro každé $a, b, c \in \mathbb{Z}$ platí, že když $a|b \wedge b|c$ pak také $a|c$. (Relace dělí je tranzitivní.)*
2. *Existují $a, b \in \mathbb{Z}$ takové, že $a|b \wedge b$ nedělí a. (Relace dělí není symetrická.)*
3. *Pro každé $a, b \in \mathbb{Z}$ platí, že $|a| = |b| \Leftrightarrow (a|b \wedge b|a)$.*
4. *Pro každé $a, b, c \in \mathbb{Z}$ platí: $ab|c \Rightarrow (a|c \wedge b|c)$.*
5. *Pro každé $a, m, n \in \mathbb{Z}$ platí, že $(a|m \wedge a|n) \Rightarrow a|(m + n)$.*
6. *Pro každé $a, b, n \in \mathbb{Z}$ platí: $a|b \Rightarrow a|nb$.*
7. *Pro každé $a, b \in \mathbb{Z} - \{0\}$ platí: $a|b \Rightarrow |a| \leq |b|$.*

Důkaz.[1]

ad 1) Pro každé $a, b, c \in \mathbb{Z}$ platí, že když $a|b \wedge b|c$, pak existují $k_1, k_2 \in \mathbb{Z}$ takové, že

$$b = k_1 a \quad \text{a} \quad c = k_2 b.$$

Když dosadíme první rovnici do druhé, dostaneme vztah $c = k_2 k_1 a$.
Vynásobením dvou celých čísel, dostaneme opět celé číslo. Takže pokud $k = k_2 \cdot k_1 \in \mathbb{Z}$, tak $c = k \cdot a$. A to podle Definice 2.1 znamená, že $a|c$.

ad 2) Chceme nalézt $a, b \in \mathbb{Z}$ tak, aby platilo $a|b$, ale neplatilo $b|a$. Zvolme například $a = 7$ a $b = 14$. Vidíme, že $a|b$, ale b nedělí a.

ad 3) Pokud $a, b \in \mathbb{Z}$ a $|a| = |b|$, pak $a = \pm b$. Pak $(a|b \wedge b|a)$, protože $b = \pm 1 \cdot a$ a $a = \pm 1 \cdot b$. Musíme dokázat i opačnou implikaci. Takže předpokládejme, že $(a|b \wedge b|a)$. Podle Definice 2.1 existují taková čísla $k_1, k_2 \in \mathbb{Z}$, že

$$b = k_1 a \quad \text{a} \quad a = k_2 b.$$

Pokud tyto rovnosti spojíme, dostaneme vztah $b = k_1 k_2 b$.

1. Pokud $b \neq 0$: Dostaneme $1 = k_1 k_2$. To znamená, že musíme najít součin dvou čísel, který je roven jedné. Jsou pouze 2 možnosti, a to $k_1 = k_2 = 1$, nebo $k_1 = k_2 = -1$.

- Pokud $k_1, k_2 = 1$:
  $b = k_1 a = 1 \cdot a = a$, $a = k_2 b = 1 \cdot b = b$. Z toho vyplývá, že $a = b$.
- Pokud $k_1, k_2 = -1$:
  $b = k_1 a = -1 \cdot a = -a$, $a = k_2 b = -1 \cdot b = -b$. Z toho vyplývá, že $|a| = |b|$.

2. Pokud $b = 0$: Z předpokladu $(a|b \wedge b|a)$ dostaneme tvrzení, že $0|a$. To znamená, že $a = k \cdot 0 = 0$. Tudíž $|a| = |b| = 0$.

ad 4) Mějme $a, b, c \in \mathbb{Z}$. Jestliže $ab|c$, pak podle Definice 2.1 musí existovat takové číslo $k \in \mathbb{Z}$, že $c = k \cdot ab$.
Označme

$$n_1 = k \cdot a \quad \text{a} \quad n_2 = k \cdot b.$$

Když dosadíme n_1 a n_2 do rovnosti $c = k \cdot ab$ obdržíme následující vztahy

$$c = n_1 \cdot b \quad \text{a} \quad c = n_2 \cdot a.$$

To znamená, že c je násobek čísla a a zároveň i čísla b. Tudíž podle Definice 2.1 můžeme říct, že $a|c \wedge b|c$.

ad 5) Jestliže $a|m$ a také $a|n$, pak m i n jsou násobky čísla a. To znamená, že existují taková čísla $k_1, k_2 \in \mathbb{Z}$, že

$$m = k_1 \cdot a \quad \text{a} \quad n = k_2 \cdot a.$$

Pak

$$m + n = k_1 \cdot a + k_2 \cdot a = (k_1 + k_2) \cdot a = k \cdot a,$$

kde $k = k_1 + k_2 \in \mathbb{Z}$.
Z předchozí rovnosti vyplývá, že číslo $m + n$ je násobek čísla a, a proto $a|m + n$.

ad 6) Pro každé $a, b, n \in \mathbb{Z}$ platí: $a|b \Rightarrow b = k \cdot a$, kde $k \in \mathbb{Z} \Rightarrow nb = n \cdot k \cdot a = k^* \cdot a$, kde $k^* = n \cdot k \in \mathbb{Z} \Rightarrow a|nb$.

ad 7) Pro každé $a, b \in \mathbb{Z} - \{0\}$ platí, že $a|b \Rightarrow b = k \cdot a$, kde $k \in \mathbb{Z} - \{0\}$. To znamená, že $|b| = |k| \cdot |a|$. Jelikož $k \in \mathbb{Z} - \{0\}$, tak musí platit $|k| \geq 1$. Z čehož vyplývá, že

$$|b| = |k| \cdot |a| \geq 1 \cdot |a| = |a|.$$

■

2.2 Největší společný dělitel

Definice 2.2 [1] *Společným dělitelem čísel $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ nazveme každé $d \in \mathbb{Z}$ splňující podmínku, že*

$$d|a_1, d|a_2, \ldots, d|a_n.$$

Mějme daná dvě libovolná celá čísla a, b. Pokud chceme nalézt společného dělitele těchto čísel, tak podle Definice 2.2 najdeme všechny dělitele obou čísel. Poté z nich vybereme jen ty společné.

Příklad 2.3
Najděte společné dělitele čísel 16 a 24.

Nejprve si vypíšeme dělitele obou čísel:

$$\begin{aligned} 16 &= \pm 1, \pm 2, \pm 4, \pm 8, \pm 16 \\ 24 &= \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24 \end{aligned}$$

Takže společnými děliteli čísel 16 a 24 jsou čísla $\pm 1, \pm 2, \pm 4$ a ± 8.

Definice 2.3 (Největší společný dělitel) [1] *Největším společným dělitelem čísel $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ je takové číslo d, které splňuje následující podmínky:*

1. $d \geq 0$
2. *Číslo d je společným dělitelem čísel $a_1, a_2, \ldots, a_n$, to znamená, že $d|a_1, d|a_2, \ldots, d|a_n$.*
3. *Jestliže nějaké celé číslo d^* je dělitelem čísel $a_1, a_2, \ldots, a_n$, potom $d^*|d$.*

Největšího společného dělitele čísel $a_1, a_2, \ldots, a_n$ označíme jako $d = gcd\,(a_1, a_2, \ldots, a_n)$.

Z předchozí definice vyplývá, že největším společným dělitelem čísel $a_1, a_2, \ldots, a_n$ je vždy to největší nezáporné číslo, které je společným dělitelem všech čísel a zároveň jej všichni ostatní dělitelé dělí.

Definice 2.4 *Celá čísla $a, b \in \mathbb{Z}$ nazýváme* nesoudělná, *je-li jejich největší společný dělitel roven 1, tzn. $gcd(a, b) = 1$. Pokud jejich největší společný dělitel je různý od 1, tzn. $gcd(a, b) \neq 1$, říkáme, že celá čísla jsou* soudělná.

V následujícím příkladu podle Definice 2.3 nalezneme největšího společného dělitele čísel 16 a 24.

Příklad 2.4
Ověřte podle definice, že $gcd(16, 24) = 8$.

Řešení:

1. $8 \geq 0$
2. $8|16$ a také $8|24$
3. Společnými děliteli čísel 16 a 24 jsou čísla $\pm 1, \pm 2, \pm 4$ a ± 8 a zároveň jsou všechna tato čísla děliteli čísla 8.

Číslo 8 tak splňuje všechny podmínky z Definice 2.3 o největším společném děliteli, a proto je největším společným dělitelem čísel 16 a 24.

Příklad 2.5
Dokažte, že $gcd(a, 0) = a$ pro každé $a \geq 0$ a ukažte, že čísla a a 0 mají právě jednoho největšího společného dělitele.

Řešení: Podle Definice 2.3 musí být největší společný dělitel čísel a a 0 nezáporné číslo a zároveň společným dělitelem obou čísel.

Nezáporní společní dělitelé obou čísel tvoří množinu D. Do této množiny patří i číslo a, které je dělitelné všemi prvky z množiny D.

Číslo a splňuje všechny podmínky z Definice 2.3, a proto $gcd(a, 0) = a$. Všechna ostatní čísla z množiny D nejsou dělitelná číslem $a \in D$, pokud $a \geq 0$, a proto nemohou být největším společným dělitelem čísel a a 0.

Věta 2.1 *Pro každá dvě čísla $a, b \in \mathbb{Z}$ existuje nejvýše jeden jejich největší společný dělitel.*

Důkaz.[1] Věta 2.1 je splněna, pokud alespoň jedno z čísel a a b je rovno nule (viz Příklad 2.5). Takže důkaz provedeme pro čísla $a, b \neq 0$.

Mějme čísla $a, b \in \mathbb{Z}$, kde $a, b \neq 0$. Předpokládejme, že $d_1 = gcd(a, b)$ i $d_2 = gcd(a, b)$. Jelikož $a, b \neq 0$, musí být $d_1, d_2 \geq 1$. Číslo d_1 je největším společným dělitelem čísel a a b. Podle Definice 2.3 jej musí dělit všichni ostatní dělitelé čísel a, b, tudíž i číslo d_2. Dostaneme $d_2|d_1$ a z Lemmatu 2.2 vyplývá, že

$$d_2 \leq d_1. \tag{1}$$

Analogicky, pokud si zvolíme d_2 jako největší společný dělitel čísel a, b, pak podle Definice 2.3 jej musí dělit všichni ostatní dělitelé čísel a, b, tedy i číslo d_1. Dostaneme $d_1|d_2$ a podle Lemmatu 2.2 platí, že

$$d_1 \leq d_2. \tag{2}$$

Z (1) a (2) vyplývá, že

$$d_1 = d_2.$$

■

2.2.1 Euklidův algoritmus

Euklidův algoritmus slouží k výpočtu největšího společného dělitele dvou přirozených čísel a a b.

Abychom se naučili určit $gcd(a, b)$ pomocí Euklidova algoritmu, musíme vědět, jak se dělí čísla se zbytkem na množině celých čísel.

Věta 2.2 [3] *Mějme dána dvě čísla $a, b \in \mathbb{Z}$, kde $b \neq 0$. Pak existují jednoznačně daná čísla $q, r \in \mathbb{Z}$ splňující následující podmínky:*

1. $a = q \cdot b + r$
2. $0 \leq r < |b|$

Číslo r nazveme zbytkem po dělení čísel a a b.

Důkaz.[3] Nejdříve ukážeme existenci čísel q, r. Platí, že $(-q) \cdot (-b) = q \cdot b$ a tudíž budeme předpokládat, že $b > 0$. Rozlišíme dva případy:

1. $a \geq 0$:

- Zde musíme rozlišit také dva případy:

  a) $a < b$, pak $a = 0 \cdot b + a$ a platí:

  $$0 \leq a < b$$

  b) $a \geq b$, pak existuje $q = [\frac{a}{b}]$ a platí:

  $$\begin{aligned} q &\leq \tfrac{a}{b} < q + 1 \\ q \cdot b &\leq a < q \cdot b + b \\ 0 &\leq a - q \cdot b < b \end{aligned}$$

  Proto $a = q \cdot b + r$ splňuje $0 \leq r < b$.

2. $a < 0$:

- Již víme, že existují čísla $r', q' \in \mathbb{Z}$ taková, že $(-a) = q' \cdot b + r'$ a $0 \leq r' < b$.
- Pokud $r' = 0$, pak $q = (-q')$ a $r = 0$, protože platí $a = (-q') \cdot b + 0$.
- Pokud $r' > 0$, pak $q = (-q') - 1$ a $r = b - r'$, protože platí

$$a = (-q' - 1) \cdot b + (b - r') \quad \text{a} \quad 0 < (b - r') < b.$$

Ještě musíme dokázat jednoznačnost čísel q a r. Budeme předpokládat, že číslo a je vyjádřeno dvěma způsoby, tj. existují taková celá čísla q_1, q_2, r_1, r_2, že platí:

$$\begin{aligned} a &= q_1 \cdot b + r_1, \text{ kde } 0 \leq r_1 < b, \\ a &= q_2 \cdot b + r_2, \text{ kde } 0 \leq r_2 < b. \end{aligned}$$

Pak platí

$$q_1 \cdot b + r_1 = q_2 \cdot b + r_2 \Rightarrow (q_1 - q_2) \cdot b = r_2 - r_1.$$

Podle výše uvedených podmínek $|r_2 - r_1| < b$, takže $|(q_1 - q_2) \cdot b| < b$ a to znamená, že

$$q_1 = q_2 \quad \Rightarrow \quad r_1 = r_2.$$

■

Nyní, když podle Věty 2.4 umíme dělit se zbytkem v oboru celých čísel, můžeme přejít k Euklidovu algoritmu.

Věta 2.3 (Euklidův algoritmus) [3] *Mějme dvě čísla $a, b \in \mathbb{N}$, kdy $a \geq b > 0$. Označme $b = b_0$ a dělením se zbytkem vytvoříme posloupnost přirozených čísel $b_1, b_2, ..., b_n$:*

$$\begin{aligned} a &= q_0 \cdot b_0 + b_1 \\ b_0 &= q_1 \cdot b_1 + b_2 \\ b_1 &= q_2 \cdot b_2 + b_3 \dots \end{aligned}$$

Dokud není $b_n = 0$. Pak $gcd(a, b) = b_{n-1}$, tj. poslední nenulový zbytek.

Důkaz Euklidova algoritmu nalezneme v [3].

Příklad 2.6
Pomocí Euklidova algoritmu najděte největšího společného dělitele:

1. gcd(140,15) = ?

$$\begin{aligned} 140 &= 9 \cdot 15 + 5 \\ 15 &= 3 \cdot 5 + 0 \end{aligned} \qquad gcd(140, 15) = 5$$

2. gcd(362,301) = ?

$$\begin{aligned} 362 &= 1 \cdot 301 + 61 \\ 301 &= 4 \cdot 61 + 57 \\ 61 &= 1 \cdot 57 + 4 \\ 57 &= 14 \cdot 4 + 1 \\ 4 &= 1 \cdot 4 + 0 \end{aligned} \qquad gcd(362, 301) = 1$$

3. gcd(158,72) = ?

$$\begin{aligned} 158 &= 2 \cdot 72 + 14 \\ 72 &= 5 \cdot 14 + 2 \\ 14 &= 7 \cdot 2 + 0 \end{aligned} \qquad gcd(158, 72) = 2$$

Věta 2.4 [1] *Nechť $a, b \in \mathbb{Z}$. Potom existují $x_0, y_0 \in \mathbb{Z}$ taková, že*

$$gcd(a, b) = x_0 a + y_0 b.$$

Důkaz. Důkaz plyne z Euklidova algoritmu. Největší společný dělitel čísel a a b, neboli $gcd(a, b)$, lze zpětně vyjádřit jako lineární kombinaci čísel a a b. ■

2.2.2 Kanonický rozklad přirozeného čísla

Největšího společného dělitele můžeme nalézt i pomocí tzv. kanonických rozkladů přirozených čísel. Jedná se o rozklady čísel na součin prvočísel. Definici tohoto pojmu uvádíme níže.

Definice 2.5 (O prvočíselnosti) [1] *Číslo $p \in \mathbb{N}$, $p \geq 2$ nazveme prvočíslem na množině přirozených čísel, právě tehdy, když pro každé $a \in \mathbb{N}$ platí:*

$$a|p \Leftrightarrow (a = 1 \vee a = p).$$

Z definice vyplývá, že prvočíslem jsou všechna přirozená čísla různá od jedničky, která jsou dělitelná pouze číslem 1 a sebou samým. Můžeme si také všimnout, že číslo 1 nepovažujeme za prvočíslo.

Příklad 2.7
Rozhodněte, zda čísla 5 a 10 jsou prvočísla.

A: Pro $p = 5$:

1. Dokážeme, že $(a = 1 \vee a = 5) \Rightarrow a|5$. Tato implikace jistě platí, protože pro každé $p \in \mathbb{N} : 1|p \wedge p|p$ podle Lemmatu 2.1.
2. Dokážeme implikaci $a|5 \Rightarrow (a = 1 \vee a = 5)$. Logicky ekvivalentní je tvrzení $(a \neq 1 \wedge a \neq 5) \Rightarrow a$ *nedělí* 5. Proto stačí ukázat, že čísla jiná než 1 a 5 nejsou děliteli čísla 5.
   Podle Lemmatu 2.2 čísla $a > p$ jistě číslo p nedělí.
   Zbývá ukázat, že čísla $\{2, 3, ..., p-1\}$ nedělí p. Číslo 2 *nedělí* 5, protože $5 = 2,5 \cdot 2$ a $2,5 \notin \mathbb{Z}$, číslo 3 *nedělí* 5, protože $5 = \frac{5}{3} \cdot 3$ a $\frac{5}{3} \notin \mathbb{Z}$, číslo 4 *nedělí* 5, protože $5 = \frac{5}{4} \cdot 5$ a $\frac{5}{4} \notin \mathbb{Z}$.
3. Z předchozích dvou bodů vyplývá, že číslo 5 je prvočíslo.

B: Pro $p = 10$:

1. Ukážeme, že $(a = 1 \vee a = 10) \Rightarrow a|10$. Tato implikace jistě platí, protože pro každé $p \in \mathbb{N} : 1|p \wedge p|p$ podle Lemmatu 2.1.
2. Ukážeme,že implikace $a|10 \Rightarrow (a = 1 \vee a = 10)$ neplatí. Například pro $a = 2$ platí, že $a|10$, ale $a \neq 1 \wedge a \neq 10$.
3. V předchozím bodě jsme si ukázali, že implikace neplatí a že číslo 10 má kromě čísel 1 a 10 také jiné dělitele, a proto číslo 10 není prvočíslem.

Definice 2.6 [1] *Číslo $s \in \mathbb{N}$, takové, že $s = d_1 d_2$, kde $d_1, d_2 \in \mathbb{N}$, a zároveň $d_1, d_2 > 1$, nazveme číslem složeným.*

Následující Lemma říká, že každé přirozené číslo n, kdy $n \geq 2$, je buď prvočíslo nebo číslo složené.

Lemma 2.3 [1] *Číslo $n \in \mathbb{N}$, $n \geq 2$ je složené číslo právě tehdy, když není prvočíslo.*

Důkaz.[1] Musíme dokázat, že číslo $n \geq 2$ je složené číslo právě tehdy, když není prvočíslo.

Předpokládejme, že $n \geq 2$ je složené číslo. Podle Definice 2.6 se $n = d_1 d_2$, kde $d_1, d_2 \in N, d_1, d_2 > 1$. To, podle Definice 2.1 znamená, že $d_2 > 1$ dělí číslo n.
Navíc $d_2 \neq n$, protože pak by $n = d_1 d_2 = d_1 n$, a to by znamenalo, že $d_1 = 1$, což je spor. Pak ale n nemůže být prvočíslo, což vyplývá z Definice 2.5.

Nyní dokážeme, že v případě, kdy n není prvočíslo, musí být n číslem složeným. Pokud n není prvočíslo, musí existovat nějaký dělitel čísla n, který je různý od n i od 1. Označme si jej d_2. Podle Definice 2.1 můžeme psát $n = k \cdot d_2$ a nic nebrání tomu, abychom označili k jako d_1, tak dostáváme $n = d_1 d_2$. Teď se ptáme, zda může být $d_1 = 1$? Pokud ano, platilo by, že $n = 1 \cdot d_2 = d_2$, což je spor s tím, že $d_2 \neq n$.

Nakonec jsme tedy zjistili, že $n = d_1 d_2$, kde d_1 a d_2 jsou přirozená čísla různá od 1, proto $d_1, d_2 > 1$. Podle Definice 2.6 musí být n číslo složené a to jsme chtěli dokázat. ∎

Ještě si ukážeme a dokážeme, že každé přirozené číslo, které je větší, nebo rovno dvěma, můžeme napsat jako součin prvočísel.

Lemma 2.4 [1] *Číslo $n \in \mathbb{N}$, $n \geq 2$ je rovno součinu prvočísla a přirozeného čísla. To znamená, že pro každé $n \in \mathbb{N}$ existují taková čísla p, $k \in \mathbb{N}$, kde p je prvočíslo, k přirozené číslo a platí rovnost*

$$n = p \cdot k.$$

Důkaz.[1] Důkaz provedeme silnou indukcí. Pro $n = 2 = 2 \cdot 1$ je tvrzení dokazovaného lemmatu pravdivé.

Budeme předpokládat, že každé číslo větší než 2 a zároveň menší než n, je součinem prvočísla a přirozeného čísla. Dokážeme, že za tohoto předpokladu je číslo n také součinem prvočísla a přirozeného čísla.

- Pokud n je prvočíslo, pak $p = n$ a $k = 1$, a tak $n = p \cdot k$.

- Pokud n není prvočíslo, pak musí být číslem složeným, což vyplývá z Lemma 2.3.

Podle Definice 2.6 (definice složeného čísla) existují přirozená čísla p_1, k_1, kde p_1, $k_1 > 1$ takové, že

$$n = p_1 \cdot k_1.$$

Navíc $2 \leq p_1 < n$. Podle předpokladu můžeme číslo p_1 napsat ve tvaru $p_1 = p \cdot k_2$, kde p je prvočíslo. Tudíž

$$n = p \cdot k_2 \cdot k_1 = p \cdot k,$$

kde $k = k_2 \cdot k_1$ je přirozené číslo. ∎

Již se pomalu dostáváme k pojmu *kanonický rozklad přirozeného čísla*. Teď, když už známe definice prvočísla a složeného čísla, dokážeme, že každé přirozené číslo, které je větší, nebo rovno dvěma, můžeme napsat jako součin prvočísel.

Příklad 2.8
Napište číslo 72 a 140 jako součin prvočísel.

$$\begin{aligned} 72 &= 2 \cdot 36 = 2 \cdot 2 \cdot 18 = 2 \cdot 2 \cdot 2 \cdot 9 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^3 \cdot 3^2 \\ 140 &= 2 \cdot 70 = 2 \cdot 2 \cdot 35 = 2 \cdot 2 \cdot 5 = 2 \cdot 2 \cdot 5 \cdot 7 = 2^2 \cdot 5 \cdot 7 \end{aligned}$$

Z Příkladu 2.8 vidíme, že číslo $n = 72$ a také $n = 140$ lze rozložit na součin prvočísel. A takovému rozkladu se říká *kanonický rozklad přirozeného čísla* n.

Věta 2.5 (O kanonickém rozkladu) [1] *Každé přirozené číslo* n*, kde* $n > 1$*, lze napsat jako součin prvočísel. To znamená, že pro každé přirozené číslo* $n \neq 1$ *existují prvočísla* $p_1, ..., p_s$*, taková, že platí:*

$$n = p_1 \cdot p_2 \cdots p_s.$$

Důkaz.[1] Důkaz provedeme silnou indukcí. Pro $n = 2$ je tvrzení dokazovaného lemmatu jistě pravdivé ($p_1 = 2$, $s = 1$).

Budeme předpokládat, že tvrzení je pravdivé pro všechna přirozená čísla větší, nebo rovna číslu 2 a menší než n. Ukážeme, že potom také číslo n je součinem prvočísel.

Podle Lemmatu 2.4, každé přirozené číslo $n > 1$ můžeme napsat ve tvaru $n = p \cdot k$, kde p je prvočíslo a k je přirozené číslo.

Pokud $k = 1$, pak $n = p = p_1$.

Pokud $k > 1$, tak z rovnosti $n = p \cdot k$ vyplývá, že $2 \leq k < n$. Pak podle indukčního předpokladu můžeme napsat číslo k jako součin prvočísel.

Takže $n = p \cdot k = p_1 \cdot p_2 \cdot ... \cdot p_s$. ∎

Lemma 2.5 [2] *Nechť* $p, a, b \in \mathbb{N}$*. Pokud* $p|ab$ *a* $gcd(p, b) = 1$*, pak* $p|a$*.*

Důkaz. Podle Věty 2.4 existují $x_0, y_0 \in \mathbb{Z}$:

$$\begin{aligned} x_0 p + y_0 b &= 1 \\ a x_0 p + y_0 ab &= a \end{aligned}$$

odtud

$$p|ab \Rightarrow ab = k \cdot p$$

proto

$$\begin{aligned} a x_0 p + y_0 kp &= a \\ p(a x_0 + y_0 k) &= a. \end{aligned}$$

Z toho vyplývá, že $p|a$. ∎

Existuje jedna chytrá věta - říká se ji *Základní věta aritmetiky*. Ta říká, že kanonický rozklad daného přirozeného čísla n existuje, až na pořadí činitelů, právě jeden. Žádné další kanonické rozklady téhož přirozeného čísla neexistují.

Věta 2.6 (Základní věta aritmetiky) [1] *Každé přirozené číslo n, které je větší než 1, lze zapsat, až na pořadí činitelů, jako součin prvočísel jediným způsobem.*

Důkaz. [1] Pokud n je prvočíslo, pak podle definice prvočíselnosti nelze n napsat jako součin jiných prvočísel. Z toho vyplývá, že jeho rozklad je jednoznačný.

Předpokládejme, že číslo n je číslo složené.

Mějme $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_l$, kde $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_l$ jsou prvočísla. Jelikož n je číslo složené, tak platí, že $k, l \geq 2$ a podle vlastnosti prvočísel (Lemma 2.5) $p_1 | (q_1 \cdot q_2 \cdot \ldots \cdot q_l)$, tudíž p_1 dělí alespoň jedno q_i z prvočísel $q_1, q_2, \ldots, q_l$.

Při vhodném přeindexování čísel $q_1, q_2, \ldots, q_l$ dostáváme rovnost

$$p_1 \cdot p_2 \cdot \ldots \cdot p_k = p_1 \cdot q_2 \cdot \ldots \cdot q_l$$
$$p_2 \cdot \ldots \cdot p_k = q_2 \cdot \ldots \cdot q_l$$

Pokud tento postup zopakujeme ještě $k-$krát, tak zjistíme, že pro každé $i \in \{1, \ldots, k\}$ existuje $j_i \in \{1, \ldots, l\}$ takové, že $p_i = q_{j_i}$ a nakonec získáme rovnost

$$1 = q_{l-k} \cdot \ldots \cdot q_l.$$

Z toho vyplývá, že

$$l = k \quad \text{a} \quad \{p_1, p_2, \ldots, p_k\} = \{q_1, q_2, \ldots, q_l\}.$$

■

Příklad 2.9
Najděte $gcd(24, 36, 60) = ?$ pomocí kanonického rozkladu přirozených čísel.

Řešení: Nejprve u všech čísel provedeme kanonický rozklad.

$$\begin{aligned} 24 &= 2 \cdot 12 = 2 \cdot 2 \cdot 6 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3 \\ 36 &= 2 \cdot 18 = 2 \cdot 2 \cdot 9 = 2 \cdot 2 \cdot 3 \cdot 3 = 2^2 \cdot 3^2 \\ 60 &= 2 \cdot 30 = 2 \cdot 2 \cdot 15 = 2 \cdot 2 \cdot 3 \cdot 5 = 2^2 \cdot 3 \cdot 5 \end{aligned}$$

Když jsme úspěšně provedli kanonický rozklad čísel, tak do součinu sepíšeme všechny společné prvočísla, která se v kanonických rozkladech čísel 24, 36 a 60 vyskytla a poté k nim připíšeme jejich nejnižší mocniny.
Takže

$$gcd(24, 36, 60) = 2^2 \cdot 3 = 12.$$

Je zřejmé, že číslo 12 je dělitelem čísel 24, 36 a 60 a také všichni společní dělitelé čísel 24, 36 a 60 jej dělí.

2.3 Nejmenší společný násobek

Definice 2.7 [1] *Nejmenším společným násobkem čísel $a, b \in \mathbb{Z}$ (značíme $n(a, b)$) je takové číslo $n \in \mathbb{Z}$, které musí splňovat následující podmínky:*

1. $n(a, b) \geq 0$
2. $a|n(a, b) \wedge b|n(a, b)$ *(tzn. $n(a, b)$ je společným násobkem čísel a a b).*
3. *Pokud $(a|k) \wedge (b|k)$, pak $n(a, b)|k$ (tzn. číslo $n(a, b)$ musí dělit všechny společné násobky čísel a, b).*

Mějme dvě libovolně velká celá čísla a, b. Pokud chceme podle Definice 2.7 nalézt nejmenší společný násobek těchto čísel, najdeme si všechny násobky obou čísel a poté z nich vybereme jejich společné násobky. Nejmenší z těchto společných násobků je roven $n(a, b)$, neboť jistě dělí všechny ostatní.

Nejmenší společný násobek libovolných čísel $a, b \in \mathbb{Z}$ můžeme snadněji najít pomocí $gcd(a, b)$ a následující věty.

Věta 2.7 [1] *Mějme dvě čísla $a, b \in \mathbb{Z} - \{0\}$. Potom platí*

$$n(a, b) = \frac{|ab|}{gcd(a,b)}.$$

Důkaz.[1] Jelikož víme, že $|ab| > 0$, tak i $gcd(a, b) > 0$ a celý zlomek $\frac{|ab|}{gcd(a,b)} > 0$.
Z Definice 2.3 víme, že $gcd(a, b)|a \wedge gcd(a, b)|b$.
Takže existují taková čísla $k_1, k_2 \in \mathbb{Z} - \{0\}$, že

$$a = k_1 \cdot gcd(a, b) \quad \text{a} \quad b = k_2 \cdot gcd(a, b).$$

Označme

$$x = \frac{|ab|}{gcd(a,b)}$$

a upravme

$$x = \frac{|ab|}{gcd(a,b)} = \frac{|k_1| \cdot gcd(a,b) \cdot |b|}{gcd(a,b)} = |k_1| \cdot |b| = k_1 \cdot b$$

a zároveň

$$x = \frac{|ab|}{gcd(a,b)} = \frac{|k_2| \cdot gcd(a,b) \cdot |a|}{gcd(a,b)} = |k_2| \cdot |a| = k_2 \cdot a.$$

Z toho vyplývá, že x je společným násobkem čísel a, b, protože $a|x \wedge b|x$. Ještě musíme dokázat, že x je nejmenším společným násobkem čísel a a b.

Předpokládejme, že n je nějaký nenulový společný násobek čísel a a b. Tzn. existují čísla $k_3, k_4 \in \mathbb{Z} - \{0\}$ taková, že

$$n = k_3 a \quad \text{a} \quad n = k_4 b.$$

Musíme dokázat, že $x|n$. Podle Věty 2.4 můžeme $gcd(a,b)$ napsat jako

$$x_0 \cdot a + y_0 \cdot b, \quad x_0, y_0 \in \mathbb{Z}.$$

S využitím výše uvedených vztahů sestavíme rovnost

$$\begin{aligned} x &= \tfrac{|ab|}{gcd(a,b)} \\ |ab| &= x \cdot gcd(a,b) \\ |ab| &= x(x_0 a + y_0 b) \\ |k_3 a \cdot k_4 b| &= x|x_0 k_3 k_4 a + y_0 k_3 k_4 b| \\ n^2 &= x|x_0 k_4 n + y_0 k_3 n| \\ |n| &= x|x_0 k_4 + y_0 k_3| \end{aligned}$$

A tímto jsme dokázali, že $x|n$. ∎

Příklad 2.10
Pomocí Věty 2.7 určíme $n(a,b)$, kde $a = 156$ a $b = 35$.

Řešení: Nejprve pomocí Euklidova algoritmu určíme $gcd(a,b)$:

$$\begin{aligned} 156 &= 4 \cdot 35 + 16 \\ 35 &= 2 \cdot 16 + 3 \\ 16 &= 5 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

Posledním nenulovým zbytkem v Euklidově algoritmu je číslo 1 a to je největší společný dělitel čísel 156 a 35. Tudíž $gcd(a,b) = 1$.

Podle Věty 2.7 vypočítáme nejmenší společný násobek

$$n(a,b) = \tfrac{|ab|}{gcd(a,b)} = \tfrac{156 \cdot 35}{gcd(156,35)} = \tfrac{5460}{1} = 5460.$$

Takže nejmenším společným násobkem čísel 156 a 35 je číslo 5460.

Nejmenší společný násobek můžeme určit také pomocí kanonického rozkladu čísel. Ukážeme si to v následujícím příkladu.

Příklad 2.11
Pomocí kanonického rozkladu čísel a a b určete $n(a,b)$, jestliže $a = 2^3 \cdot 5^2 \cdot 7^3$ a $b = 3^4 \cdot 5^3 \cdot 7^2$.

Řešení: Nejprve do součinu sepíšeme všechny prvočísla, která se vyskytla v kanonických rozkladech obou čísel a poté k nim připíšeme jejich nejvyšší mocniny. Je zřejmé, že takto vzniklé číslo je nezáporné a je společným násobkem čísel a a b. Navíc každý společný násobek čísel a a b je tímto číslem dělitelný.
Takže $n(a,b) = 2^3 \cdot 3^4 \cdot 5^3 \cdot 7^3$.

3 Kongruence na množině celých čísel

3.1 Pojem binární relace

Definice 3.1 *Binární relace R na množině A je podmnožina kartézského součinu $A \times A$. Jestliže $(x, y) \in R$, pak píšeme xRy (x je v relaci R s y).*

Vlastnosti relací:

1. Symetrie

   - Binární relace R na množině A je *symetrická* právě tehdy, když pro každé $x, y \in A$ platí, pokud xRy, pak yRx.

2. Tranzitivita

   - Binární relace R na množině A je *tranzitivní* právě tehdy, když pro každé $x, y, z \in A$ platí, pokud xRy a yRz, pak xRz.

3. Reflexe

   - Binární relace R na množině A je *reflexivní* právě tehdy, když pro každé $x \in A$ platí xRx.

4. Antisymetrie

   - Binární relace R na množině A je *antisymetrická* právě tehdy, když pro každé $x, y \in A$ platí, pokud xRy a yRx, pak $x = y$.

Relace, která je reflexivní, symetrická a zároveň tranzitivní se nazývá *relace ekvivalence*. Naopak relace, která je reflexivní, antisymetrická a tranzitivní je relací částečného uspořádání. My se teď budeme zabývat relací ekvivalence.

3.1.1 Relace ekvivalence

Definice 3.2 *Binární relace R na množině A se nazývá ekvivalence, pokud platí následující podmínky:*

- *Pro každé $x \in A$: xRx*
- *Pro každé $x, y \in A$: $xRy \Rightarrow yRx$*
- *Pro každé $x, y, z \in A$: $(xRy \wedge yRz) \Rightarrow xRz$*

Důležitým příkladem ekvivalence je kongruence modulo m, které se budeme v této kapitole věnovat nejvíce.

3.2 Kongruence modulo m

Definice 3.3 *Relací kongruence na okruhu celých čísel $\mathbb{Z} = \langle \mathbb{Z}, +, \cdot \rangle$ nazveme každou relaci R na $\mathbb{Z}$ splňující následující podmínky:*

1. *R je relace ekvivalence na $\mathbb{Z}$*
2. *$\forall a, b, c, d \in \mathbb{Z} : (aRb \wedge cRd) \Rightarrow ((a + c)R(b + d) \wedge (a \cdot c)R(b \cdot d))$*

Definice 3.4 *Nechť čísla $a, b \in \mathbb{Z}$ a číslo $m \in \mathbb{N}$. Pokud existuje takové číslo $k \in \mathbb{Z}$, že platí $a - b = k \cdot m$, pak číslo a je kongruentní s b modulo m.*
Značíme

$$a \equiv b \,(\mathrm{mod} m).$$

Ukážeme, že výše uvedená definice je korektní. Dokážeme, že relace $\equiv$ je opravdu relace kongruence na množině $\mathbb{Z}$.

Nejprve si ukážeme, že $\equiv$ je relace na $\mathbb{Z}$. To dokážeme jednoduše tak, že ověříme, zda relace kongruence modulo m splňuje axiomy relace ekvivalence na množině $\mathbb{Z}$:

1. Jakékoliv celé číslo musí být kongruentní samo se sebou (tj. reflexe).
2. Pokud je celé číslo a kongruentní s celým číslem b, pak i b musí být kongruentní s a (tj. symetrie).
3. Jestliže celé číslo a je kongruentní s celým číslem b modulo m a číslo b je kongruentní s celým číslem c modulo m, pak také číslo a je kongruentní s číslem c modulo m (tj. tranzitivita).

Pokud relace kongruence splňuje tyto podmínky, pak se jedná o relaci ekvivalence na množině $\mathbb{Z}$.

Věta 3.1 *[1] Nechť čísla $a, b, c \in \mathbb{Z}$ a číslo $m \in \mathbb{N}$, pak relace kongruence modulo m je relací ekvivalence na množině $\mathbb{Z}$. Platí:*

1. *$a \equiv a \,(\mathrm{mod} m)$*
2. *$a \equiv b \,(\mathrm{mod} m) \Rightarrow b \equiv a \,(\mathrm{mod} m)$*
3. *$(a \equiv b \,(\mathrm{mod} m) \wedge b \equiv c \,(\mathrm{mod} m)) \Rightarrow a \equiv c \,(\mathrm{mod} m)$*

Důkaz.[1]

- Podle Definice 3.4, pro každé $a \in \mathbb{Z}$ platí, že $a - a = 0 \cdot m$. To znamená, že

$$a \equiv a \,(\mathrm{mod} m).$$

- Předpokládejme, že $a \equiv b \,(\mathrm{mod} m)$. Chceme-li dokázat $b \equiv a \,(\mathrm{mod} m)$, tak podle Definice 3.4 upravíme rovnost $a - b = k \cdot m$ tak, že dostaneme

  $$b - a = -k \cdot m = k_1 \cdot m,$$

  kde $k_1 \in \mathbb{Z}$. Z toho vyplývá, že $b \equiv a \,(\mathrm{mod} m)$.

- Budeme předpokládat, že $a \equiv b \,(\mathrm{mod} m) \wedge b \equiv c \,(\mathrm{mod} m)$. Podle Definice 3.4 dostaneme

  $$\begin{aligned} a - b &= k_1 \cdot m \\ b - c &= k_2 \cdot m \end{aligned}$$

  Výše uvedené rovnosti sečteme a dostaneme

  $$a - c = (k_1 - k_2) \cdot m = k \cdot m,$$

  kde $k \in \mathbb{Z}$.
  Podle Definice 3.4 je zřejmé, že $a \equiv c \,(\mathrm{mod} m)$.

■

Dále ukážeme, že relace kongruence modulo m splňuje i druhou podmínku z definice relace kongruence.

Věta 3.2 *Nechť $a, b, c, d \in \mathbb{Z}, m \in \mathbb{N}$. Jestliže $a \equiv b \,(\mathrm{mod} m)$ a $c \equiv d \,(\mathrm{mod} m)$, pak platí:*

1. $a + c \equiv b + d \,(\mathrm{mod} m)$
2. $a - c \equiv b - d \,(\mathrm{mod} m)$
3. $a \cdot c \equiv b \cdot d \,(\mathrm{mod} m)$

Důkaz. Předpokládejme, že $a \equiv b \,(\mathrm{mod} m)$ a $c \equiv d \,(\mathrm{mod} m)$.

1. $\begin{aligned} &a - b = k_1 m \\ &\underline{c - d = k_2 m} \\ &(a + c) - (b + d) = (k_1 + k_2) \cdot m \Rightarrow a + c \equiv b + d \,(\mathrm{mod} m) \end{aligned}$
2. $\begin{aligned} &a - b = k_1 m \\ &\underline{c - d = k_2 m} \\ &(a - c) - (b - d) = (k_1 - k_2) \cdot m \Rightarrow a - c \equiv b - d \,(\mathrm{mod} m) \end{aligned}$
3. $\begin{aligned} &a - b = k_1 m \\ &\underline{c - d = k_2 m} \\ &(a \cdot c) - (b \cdot d) = (a - b) \cdot c + (c - d) \cdot b \equiv (c \cdot k_1 + b \cdot k_2) m \end{aligned}$

   Jelikož $c \cdot k_1 + b \cdot k_2$ reprezentuje nějaké celé číslo, tak platí

   $$a \cdot c \equiv b \cdot d \,(\mathrm{mod} m).$$

■

Věta 3.3 *Nechť $a, b, c \in \mathbb{N}$, $gcd(c, m) = 1$. Potom platí*

$$a \cdot c \equiv b \cdot c \,(\mathrm{mod} m) \Rightarrow a \equiv b \,(\mathrm{mod} m).$$

Důkaz. Předpokládejme, že

$$a \cdot c \equiv b \cdot c \,(\mathrm{mod} m) \Rightarrow (a \cdot c) - (b \cdot c) = k \cdot m,$$

kde $k \in \mathbb{Z}$.

$$c \cdot (a - b) = k \cdot m \Rightarrow m | c \cdot (a - b).$$

Z Lemma 2.5 plyne, že

$$m | (a - b) \Rightarrow a - b = k_1 \cdot m,$$

kde $k_1 \in \mathbb{Z}$ a tak

$$a \equiv b \,(\mathrm{mod} m).$$

■

3.3 Malá Fermatova věta

Pro tvorbu kritéria dělitelnosti prvočíslem p využijeme malou Fermatovu větu.

Věta 3.4 (Malá Fermatova věta) [2] *Nechť $p \in \mathbb{N}$ je prvočíslo. Pak pro všechna přirozená čísla a, která jsou nesoudělná s p platí*

$$a^{p-1} \equiv 1 \,(\mathrm{mod} p).$$

Důkaz. Nechť $a \in \mathbb{N}$, $gcd(a, p) = 1$. Jestliže pro nějaké $i, j \in \{1, 2, \ldots, p-1\}$ platí

$$i \cdot a \equiv j \cdot a \,(\mathrm{mod} p).$$

Pak podle Věty 3.3

$$i \equiv j \,(\mathrm{mod} p).$$

Protože $i, j \in \{1, 2, \ldots, p-1\}$ musí platit $i = j$. Z toho plyne, že čísla z množiny $\{a, 2a, \ldots, (p-1)a\}$ nejsou navzájem kongruentní modulo p.
Každé z čísel $a, 2a, \ldots, (p-1)a$ patří do jiné ze zbytkových tříd $1, 2, \ldots, (p-1) \,(\mathrm{mod} p)$.
Proto

$$a \cdot 2a \cdot \cdots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \cdots \cdot (p-1) \,(\mathrm{mod} p).$$

Každé z čísel $1, 2, \ldots, (p-1)$ je nesoudělné s p a proto

$$a^{p-1} \equiv 1 \,(\mathrm{mod} p).$$

■

4 Kritéria dělitelnosti

V této kapitole využijeme znalostí z předchozích kapitol a budeme se věnovat určitým pravidlům, týkajících se dělitelnosti.

Abychom mohli snadno rozhodnout, zda je nějaké přirozené číslo dělitelné beze zbytku jiným přirozeným číslem existují tzv. *Kritéria dělitelnosti*.

My si ukážeme ty nejzákladnější.

4.1 Kritéria v desítkové soustavě

V této části 4. kapitoly budeme zkoumat dělitelnost přirozeného čísla n, jehož ciferný zápis v desítkové soustavě je $a_k a_{k-1} \dots a_0$. To znamená, že

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0,$$

kde $\forall i \in \{k, k-1, \dots, 0\} : a_i \in \{0, 1, \dots, 9\}; a_k \neq 0$.

4.1.1 Dělitelnost dvěma

Tvrzení 4.1 *Číslo $n \in \mathbb{N}$ je dělitelné dvěma právě tehdy, když poslední cifra čísla n je sudá (tj. $0, 2, 4, 6, 8$).*

Důkaz. Nechť n je přirozené číslo a $a_k a_{k-1} \dots a_0$ je jeho ciferný zápis, tzn.

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0.$$

Uvažme, že

$$\begin{aligned} 10^1 &\equiv 0 \,(\mathrm{mod} 2) \\ 10^2 &\equiv 0 \,(\mathrm{mod} 2) \\ 10^3 &\equiv 0 \,(\mathrm{mod} 2) \\ &\vdots \end{aligned}$$

Indukcí je možné snadno dokázat, že

$$\forall k \in \mathbb{N} : \quad 10^k \equiv 0 \,(\mathrm{mod} 2).$$

Číslo n je dělitelné dvěma právě tehdy, když

$$\begin{aligned} 2 \mid n \quad &\Leftrightarrow \quad n \equiv 0 \,(\mathrm{mod} 2) \\ &\Leftrightarrow \quad a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 \equiv 0 \,(\mathrm{mod} 2) \\ &\Leftrightarrow \quad a_k \cdot 0 + a_{k-1} \cdot 0 + \cdots + a_1 \cdot 0 + a_0 \equiv 0 \,(\mathrm{mod} 2) \\ &\Leftrightarrow \quad a_0 \equiv 0 \,(\mathrm{mod} 2) \end{aligned} \tag{3}$$

Z (3) tak plyne, že

$$2 \mid n \Leftrightarrow 2 | a_0, \quad a_0 \in \{0, 2, 4, 6, 8\}.$$

■

Příklad 4.1
Určete, zda číslo 644 je dělitelné číslem 2.

$644 = 6 \cdot 10^2 + 4 \cdot 10^1 + 4$

Z důkazu Tvrzení 4.1 plyne, že

$$\begin{array}{rcl} 2|n & \Leftrightarrow & 2|a_0 \\ 2|644 & \Leftrightarrow & 2|4 \end{array}$$

Číslo 2 *dělí* číslo 4 a to znamená, že číslo 644 je dělitelné dvěma.

4.1.2 Dělitelnost třemi

Tvrzení 4.2 *Číslo $n \in \mathbb{N}$ je dělitelné třemi právě tehdy, když jeho ciferný součet je dělitelný třemi.*

Důkaz. Nechť n je přirozené číslo a $a_k a_{k-1} \dots a_0$ je jeho ciferný zápis, tzn.

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0.$$

Uvažme, že

$$\begin{array}{rcl} 10^1 & \equiv & 1\,(\mathrm{mod}3) \\ 10^2 & \equiv & 1\,(\mathrm{mod}3) \\ 10^3 & \equiv & 1\,(\mathrm{mod}3) \\ & \vdots & \end{array}$$

Indukcí je možné snadno dokázat, že

$$\forall k \in \mathbb{N}: \quad 10^k \equiv 1\,(\mathrm{mod}3).$$

Číslo n je dělitelné třemi právě tehdy, když

$$\begin{array}{rcll} 3 \,|\, n & \Leftrightarrow & n \equiv 0\,(\mathrm{mod}3) & \\ & \Leftrightarrow & a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 \equiv 0\,(\mathrm{mod}3) & \\ & \Leftrightarrow & a_k + a_{k-1} + \ldots + a_1 + a_0 \equiv 0\,(\mathrm{mod}3) & (4) \\ & \Leftrightarrow & \sum_{i=0}^{k} a_i \equiv 0\,(\mathrm{mod}3) & \end{array}$$

Z (4) tak plyne, že

$$3 \,|\, n \Leftrightarrow 3 \,|\, \sum_{i=0}^{k} a_i.$$

■

Příklad 4.2
Určete, zda číslo 1434 je dělitelné číslem 3.

$1434 = 1 \cdot 10^3 + 4 \cdot 10^2 + 3 \cdot 10^1 + 4$

Z důkazu Tvrzení 4.2 plyne, že

$$\begin{aligned} 3|n &\Leftrightarrow 3|\sum_{i=0}^{k} a_i \\ 3|1434 &\Leftrightarrow 3|4+3+4+1 \\ &\Leftrightarrow 3|12 \end{aligned}$$

Číslo 3 *dělí* číslo 12 a to znamená, že číslo 1434 je dělitelné třemi.

4.1.3 Dělitelnost čtyřmi

Tvrzení 4.3 *Číslo $n \in \mathbb{N}$ je dělitelné čtyřmi právě tehdy, když*

$$4 \,|\, 2a_1 + a_0.$$

Důkaz. Nechť n je přirozené číslo a $a_k a_{k-1} \ldots a_0$ je jeho ciferný zápis, tzn.

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0.$$

Uvažme, že

$$\begin{aligned} 10^1 &\equiv 2\,(\mathrm{mod}4) \\ 10^2 &\equiv 0\,(\mathrm{mod}4) \\ 10^3 &\equiv 0\,(\mathrm{mod}4) \\ &\vdots \end{aligned}$$

Indukcí je možné snadno dokázat, že

$$\forall k \in \mathbb{N}, k \geq 2: \quad 10^k \equiv 0\,(\mathrm{mod}4).$$

Číslo n je dělitelné čtyřmi právě tehdy, když

$$\begin{aligned} 4 \,|\, n &\Leftrightarrow n \equiv 0\,(\mathrm{mod}4) \\ &\Leftrightarrow a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 \equiv 0\,(\mathrm{mod}4) \\ &\Leftrightarrow a_k \cdot 0 + a_{k-1} \cdot 0 + \ldots + a_1 \cdot 2 + a_0 \equiv 0\,(\mathrm{mod}4) \\ &\Leftrightarrow 2a_1 + a_0 \equiv 0\,(\mathrm{mod}4) \end{aligned} \tag{5}$$

Z (5) tak plyne, že

$$4 \,|\, n \Leftrightarrow 4 \,|\, 2a_1 + a_0.$$

■

Příklad 4.3
Určete, zda číslo 3624 je dělitelné číslem 4.

$3624 = 3 \cdot 10^3 + 6 \cdot 10^2 + 2 \cdot 10^1 + 4.$

Z důkazu Tvrzení 4.3 plyne, že

$$\begin{array}{rcl} 4|n & \Leftrightarrow & 4|2a_1 + a_0 \\ 4|3624 & \Leftrightarrow & 4|2 \cdot 2 + 4 \\ & \Leftrightarrow & 4|8 \end{array}$$

Číslo 4 *dělí* číslo 8 a to znamená, že číslo 3624 je dělitelné čtyřmi.

4.1.4 Dělitelnost pěti

Tvrzení 4.4 *Číslo $n \in \mathbb{N}$ je dělitelné pěti právě tehdy, když jeho poslední číslice je 0 nebo 5.*

Důkaz. Nechť n je přirozené číslo a $a_k a_{k-1} \ldots a_0$ je jeho ciferný zápis, tzn.

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0.$$

Uvažme, že

$$\begin{array}{rcl} 10^1 & \equiv & 0 \,(\mathrm{mod} 5) \\ 10^2 & \equiv & 0 \,(\mathrm{mod} 5) \\ 10^3 & \equiv & 0 \,(\mathrm{mod} 5) \\ & \vdots & \end{array}$$

Indukcí je možné snadno dokázat, že

$$\forall k \in \mathbb{N}: \quad 10^k \equiv 0 \,(\mathrm{mod} 5).$$

Číslo n je dělitelné pěti právě tehdy, když

$$\begin{array}{rcll} 5\,|n & \Leftrightarrow & n \equiv 0 \,(\mathrm{mod} 5) & \\ & \Leftrightarrow & a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 \equiv 0 \,(\mathrm{mod} 5) & \\ & \Leftrightarrow & a_k \cdot 0 + a_{k-1} \cdot 0 + \ldots + a_1 \cdot 0 + a_0 \equiv 0 \,(\mathrm{mod} 5) & (6) \\ & \Leftrightarrow & a_0 \equiv 0 \,(\mathrm{mod} 5) & \end{array}$$

Z (6) tak plyne, že

$$5\,|\,n \Leftrightarrow 5\,|\,a_0, \quad a_0 \in \{0, 5\}.$$

■

Příklad 4.4
Určete, zda číslo 955 je dělitelné číslem 5.

$955 = 9 \cdot 10^2 + 5 \cdot 10^1 + 5.$

Z důkazu Tvrzení 4.4 plyne, že

$$\begin{aligned} 5|n &\Leftrightarrow 5|a_0 \\ 5|955 &\Leftrightarrow 5|5 \end{aligned}$$

Číslo 5 *dělí* číslo 5 a to znamená, že číslo 955 je dělitelné pěti.

4.1.5 Dělitelnost šesti

Tvrzení 4.5 *Číslo $n \in \mathbb{N}$ je dělitelné šesti právě tehdy, když*

$$6 \mid n \Leftrightarrow \left(2|a_0 \wedge 3|\sum_{i=0}^{k} a_i \right).$$

Důkaz. Podle Tvrzení 4.1 a Tvrzení 4.2 nastane, že

$$6 \mid n \Leftrightarrow (2|n \wedge 3|n).$$

■

Tvrzení 4.6 *Číslo $n \in \mathbb{N}$ je dělitelné šesti právě tehdy, když*

$$6 \mid n \Leftrightarrow \left(4 \cdot \sum_{i=1}^{k} a_i + a_0 \right).$$

Důkaz. Nechť n je přirozené číslo a $a_k a_{k-1} \ldots a_0$ je jeho ciferný zápis, tzn.

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0.$$

Uvažme, že

$$\begin{aligned} 10^1 &\equiv 4 \,(\mathrm{mod} 6) \\ 10^2 &\equiv 4 \,(\mathrm{mod} 6) \\ 10^3 &\equiv 4 \,(\mathrm{mod} 6) \\ &\vdots \end{aligned}$$

Indukcí je možné snadno dokázat, že

$$\forall k \in \mathbb{N}: \quad 10^k \equiv 4 \,(\mathrm{mod} 6).$$

Proto

$$\begin{aligned} 6 \,|\, n &\Leftrightarrow n \equiv 0\,(\mathrm{mod}6) \\ &\Leftrightarrow a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 \equiv 0\,(\mathrm{mod}6) \\ &\Leftrightarrow a_k \cdot 4 + a_{k-1} \cdot 4 + \ldots + a_1 \cdot 4 + a_0 \equiv 0\,(\mathrm{mod}6) \\ &\Leftrightarrow 4 \cdot \sum_{i=1}^{k} a_i + a_0 \equiv 0\,(\mathrm{mod}6) \end{aligned} \tag{7}$$

Z (7) plyne, že

$$6 \,|\, n \Leftrightarrow 6 \,|\, \left(4 \cdot \sum_{i=1}^{k} a_i + a_0\right).$$

■

Příklad 4.5
Určete, zda číslo 924 je dělitelné číslem 6.

$924 = 9 \cdot 10^2 + 2 \cdot 10^1 + 4.$

Z důkazu Tvrzení 4.6 plyne, že

$$\begin{aligned} 6|n &\Leftrightarrow 6 \,|\, 4 \cdot \sum_{i=1}^{k} a_i + a_0 \\ 6|924 &\Leftrightarrow 6 \,|\, 4 \cdot 2 + 4 \cdot 9 + 4 \\ &\Leftrightarrow 6 \,|\, 48 \end{aligned}$$

Číslo 6 *dělí* číslo 48 a to znamená, že číslo 924 je dělitelné šesti.

4.1.6 Dělitelnost sedmi

Tvrzení 4.7 *Číslo $n \in \mathbb{N}$ je dělitelné sedmi právě tehdy, když*

$$\begin{aligned} 7 \,|\, n \;\Leftrightarrow\; 7 \,|\, \Bigg(&1 \cdot \sum_{i=0}^{q-1} (a_{i\cdot 6+0}) + 3 \cdot \sum_{i=0}^{q-1} (a_{i\cdot 6+1}) + 2 \cdot \sum_{i=0}^{q-1} (a_{i\cdot 6+2}) + 6 \cdot \sum_{i=0}^{q-1} (a_{i\cdot 6+3}) + \\ &+ 4 \cdot \sum_{i=0}^{q-1} (a_{i\cdot 6+4}) + 5 \cdot \sum_{i=0}^{q-1} (a_{i\cdot 6+5}) + a_{q6} \cdot 1 + a_{q6+1} \cdot 3 + \ldots + a_{q6+r} \cdot b_r \Bigg), \end{aligned}$$

kde $b_0 = 1, b_1 = 3, b_2 = 2, b_3 = 6, b_4 = 4, b_5 = 5$ *a* $k + 1 = q \cdot 6 + r$, *kde* $0 \leq r < 6$, $q \in \mathbb{Z}$.

Důkaz. Nechť n je přirozené číslo a $a_k a_{k-1} \ldots a_0$ je jeho ciferný zápis, tzn.

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0.$$

Číslo 7 je prvočíslo a tak použijeme Větu 3.4 (malá Fermatova věta) a dostaneme

$$\begin{aligned}
10^1 &\equiv 3\,(\mathrm{mod}7)\\
10^2 &\equiv 2\,(\mathrm{mod}7)\\
10^3 &\equiv 6\,(\mathrm{mod}7)\\
10^4 &\equiv 4\,(\mathrm{mod}7)\\
10^5 &\equiv 5\,(\mathrm{mod}7)\\
10^6 &\equiv 1\,(\mathrm{mod}7)\\
10^7 = 10^{1+6} &\equiv 3\,(\mathrm{mod}7)\\
10^8 = 10^{2+6} &\equiv 2\,(\mathrm{mod}7)\\
10^9 = 10^{3+6} &\equiv 6\,(\mathrm{mod}7)\\
&\vdots\\
10^{13} = 10^{1+2\cdot 6} &\equiv 3\,(\mathrm{mod}7)\\
10^{14} = 10^{2+2\cdot 6} &\equiv 2\,(\mathrm{mod}7)\\
10^{15} = 10^{3+2\cdot 6} &\equiv 6\,(\mathrm{mod}7)\\
&\vdots
\end{aligned}$$

Označme $b_0 = 1, b_1 = 3, b_2 = 2, b_3 = 6, b_4 = 4, b_5 = 5$. Jestliže $k+1 = q\cdot 6 + r$, kde $0 \le r < 6$, $q \in \mathbb{Z}$, pak

$$\begin{aligned}
7 \,|\, n \quad \Leftrightarrow \quad 7 \,|\, \Bigg(& 1\cdot\sum_{i=0}^{q-1}(a_{i\cdot 6+0}) + 3\cdot\sum_{i=0}^{q-1}(a_{i\cdot 6+1}) + 2\cdot\sum_{i=0}^{q-1}(a_{i\cdot 6+2}) + 6\cdot\sum_{i=0}^{q-1}(a_{i\cdot 6+3}) + \\
& + 4\cdot\sum_{i=0}^{q-1}(a_{i\cdot 6+4}) + 5\cdot\sum_{i=0}^{q-1}(a_{i\cdot 6+5}) + a_{q6}\cdot 1 + a_{q6+1}\cdot 3 + \ldots + a_{q6+r}\cdot b_r \Bigg).
\end{aligned}$$

■

Příklad 4.6
Určete, zda číslo 1792 je dělitelné číslem 7.

$1792 = 1\cdot 10^3 + 7\cdot 10^2 + 9\cdot 10^1 + 2.$

Z důkazu Tvrzení 4.7 plyne, že

$$\begin{aligned}
7|1792 \quad &\Leftrightarrow \quad 7 \,|\, 1\cdot 6 + 7\cdot 2 + 9\cdot 3 + 2\cdot 1\\
&\Leftrightarrow \quad 7 \,|\, 6 + 14 + 27 + 2\\
&\Leftrightarrow \quad 7 \,|\, 49
\end{aligned}$$

Číslo 7 *dělí* číslo 49 a to znamená, že číslo 1792 je dělitelné sedmi.

4.1.7 Dělitelnost osmi

Tvrzení 4.8 *Číslo $n \in \mathbb{N}$ je dělitelné osmi právě tehdy, když*

$$8 \,|\, n \Leftrightarrow 8 \,|\, 4a_2 + 2a_1 + a_0.$$

Důkaz. Nechť n je přirozené číslo a $a_k a_{k-1} \dots a_0$ je jeho ciferný zápis, tzn.

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0.$$

Uvažme, že

$$\begin{aligned} 10^1 &\equiv 2\,(\mathrm{mod}8) \\ 10^2 &\equiv 4\,(\mathrm{mod}8) \\ 10^3 &\equiv 0\,(\mathrm{mod}8) \\ 10^4 &\equiv 0\,(\mathrm{mod}8) \\ &\vdots \end{aligned}$$

Indukcí je možné snadno dokázat, že

$$\forall k \in \mathbb{N}, k \geq 3: \quad 10^k \equiv 0\,(\mathrm{mod}8).$$

Číslo n je dělitelné osmi právě tehdy, když

$$\begin{aligned} 8 \,|\, n &\Leftrightarrow n \equiv 0\,(\mathrm{mod}8) \\ &\Leftrightarrow a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 \equiv 0\,(\mathrm{mod}8) \\ &\Leftrightarrow a_k \cdot 0 + a_{k-1} \cdot 0 + \ldots + a_2 \cdot 4 + a_1 \cdot 2 + a_0 \equiv 0\,(\mathrm{mod}8) \\ &\Leftrightarrow 4a_2 + 2a_1 + a_0 \equiv 0\,(\mathrm{mod}8) \end{aligned} \tag{8}$$

Z (8) tak plyne, že

$$8|n \Leftrightarrow 8|4a_2 + 2a_1 + a_0.$$

■

Příklad 4.7
Určete, zda číslo 6384 je dělitelné číslem 8.

$6384 = 6 \cdot 10^3 + 3 \cdot 10^2 + 8 \cdot 10^1 + 4.$

Z důkazu Tvrzení 4.8 plyne, že

$$\begin{aligned} 8|n &\Leftrightarrow 8 \,|\, 4a_2 + 2a_1 + a_0 \\ 8|6384 &\Leftrightarrow 8 \,|\, 4 \cdot 3 + 2 \cdot 8 + 4 \\ &\Leftrightarrow 8 \,|\, 12 + 16 + 4 \\ &\Leftrightarrow 8 \,|\, 32 \end{aligned}$$

Číslo 8 *dělí* číslo 32 a to znamená, že číslo 6384 je dělitelné osmi.

4.1.8 Dělitelnost devíti

Tvrzení 4.9 *Číslo $n \in \mathbb{N}$ je dělitelné devíti právě tehdy, když jeho ciferný součet je dělitelný devíti.*

Důkaz. Nechť n je přirozené číslo a $a_k a_{k-1} \dots a_0$ je jeho ciferný zápis, tzn.

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0.$$

Uvažme, že

$$\begin{aligned} 10^1 &\equiv 1 \,(\mathrm{mod} 9) \\ 10^2 &\equiv 1 \,(\mathrm{mod} 9) \\ 10^3 &\equiv 1 \,(\mathrm{mod} 9) \\ &\vdots \end{aligned}$$

Indukcí je možné snadno dokázat, že

$$\forall k \in \mathbb{N}: \quad 10^k \equiv 1 \,(\mathrm{mod} 9).$$

Číslo n je dělitelné devíti právě tehdy, když

$$\begin{aligned} 9|n \quad &\Leftrightarrow \quad n \equiv 0 \,(\mathrm{mod} 9) \\ &\Leftrightarrow \quad a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 \equiv 0 \,(\mathrm{mod} 9) \\ &\Leftrightarrow \quad a_k + a_{k-1} + \ldots + a_1 + a_0 \equiv 0 \,(\mathrm{mod} 9) \\ &\Leftrightarrow \quad \sum_{i=0}^{k} a_i \equiv 0 \,(\mathrm{mod} 9) \end{aligned} \tag{9}$$

Z (9) tak plyne, že

$$9 \,|\, n \Leftrightarrow 9| \sum_{i=0}^{k} a_i.$$

■

Příklad 4.8
Určete, zda číslo 4536 je dělitelné číslem 9.

$4536 = 4 \cdot 10^3 + 5 \cdot 10^2 + 3 \cdot 10^1 + 6.$

Z důkazu Tvrzení 4.9 plyne, že

$$\begin{aligned} 9|n \quad &\Leftrightarrow \quad 9 \,|\, \textstyle\sum_{i=0}^{k} a_i \\ 9|4536 \quad &\Leftrightarrow \quad 9 \,|\, 6 + 3 + 5 + 4 \\ &\Leftrightarrow \quad 9 \,|\, 18 \end{aligned}$$

Číslo 9 *dělí* číslo 18 a to znamená, že číslo 4536 je dělitelné devíti.

4.1.9 Dělitelnost deseti

Tvrzení 4.10 *Číslo $n \in \mathbb{N}$ je dělitelné deseti právě tehdy, když jeho poslední číslice je nula.*

Důkaz. Nechť n je přirozené číslo a $a_k a_{k-1} \dots a_0$ je jeho ciferný zápis, tzn.

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0.$$

Uvažme, že

$$\begin{aligned} 10^1 &\equiv 0 \,(\mathrm{mod} 10) \\ 10^2 &\equiv 0 \,(\mathrm{mod} 10) \\ 10^3 &\equiv 0 \,(\mathrm{mod} 10) \\ &\vdots \end{aligned}$$

Indukcí je možné snadno dokázat, že

$$\forall k \in \mathbb{N}: \quad 10^k \equiv 0 \,(\mathrm{mod} 10).$$

Číslo n je dělitelné deseti právě tehdy, když

$$\begin{aligned} 10 \,|\, n \quad &\Leftrightarrow \quad n \equiv 0 \,(\mathrm{mod} 10) \\ &\Leftrightarrow \quad a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 \equiv 0 \,(\mathrm{mod} 10) \\ &\Leftrightarrow \quad a_k \cdot 0 + a_{k-1} \cdot 0 + \ldots + a_1 \cdot 0 + a_0 \equiv 0 \,(\mathrm{mod} 10) \\ &\Leftrightarrow \quad a_0 \equiv 0 \,(\mathrm{mod} 10) \end{aligned} \tag{10}$$

Z (10) tak plyne, že

$$10 \,|\, n \Leftrightarrow 10 \,|\, a_0, \quad a_0 = 0.$$

■

Příklad 4.9
Určete, zda číslo 680 je dělitelné číslem 10.

$680 = 6 \cdot 10^2 + 8 \cdot 10^1 + 0.$

Z důkazu Tvrzení 4.10 plyne, že

$$\begin{aligned} 10|n \quad &\Leftrightarrow \quad 10 \,|\, a_0 \\ 10|680 \quad &\Leftrightarrow \quad 10 \,|\, 0 \end{aligned}$$

Číslo 10 *dělí* číslo 0 a to znamená, že číslo 680 je dělitelné deseti.

4.1.10 Dělitelnost jedenácti

Tvrzení 4.11 *Číslo $n \in \mathbb{N}$ je dělitelné jedenácti právě tehdy, když rozdíl součtu číslic na sudém a lichém místě je dělitelný 11.*

Důkaz. Nechť n je přirozené číslo a $a_k a_{k-1} \dots a_0$ je jeho ciferný zápis, tzn.

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0.$$

Uvažme, že

$$\begin{aligned} 10^1 &\equiv -1 \,(\mathrm{mod} 11) \\ 10^2 &\equiv 1 \,(\mathrm{mod} 11) \\ 10^3 &\equiv -1 \,(\mathrm{mod} 11) \\ 10^4 &\equiv 1 \,(\mathrm{mod} 11) \\ &\vdots \\ 10^k &\equiv (-1)^k \,(\mathrm{mod} 11) \end{aligned}$$

Číslo n je dělitelné jedenácti právě tehdy, když

$$\begin{aligned} 11 \,|\, n \quad &\Leftrightarrow \quad n \equiv 0 \,(\mathrm{mod} 11) \\ &\Leftrightarrow \quad a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 \equiv 0 \,(\mathrm{mod} 11) \\ &\Leftrightarrow \quad a_k \cdot (-1)^k + a_{k-1} \cdot (-1)^{k-1} + \ldots + a_1 \cdot (-1) + a_0 \equiv 0 \,(\mathrm{mod} 11) \\ &\Leftrightarrow \quad a_k \cdot (-1)^k + \cdots + a_4 - a_3 + a_2 - a_1 + a_0 \equiv 0 \,(\mathrm{mod} 11) \\ &\Leftrightarrow \quad \sum_{i=0}^{k} (-1)^i \cdot a_i \equiv 0 \,(\mathrm{mod} 11) \end{aligned} \tag{11}$$

Z (11) tak plyne, že

$$11 \,|\, n \Leftrightarrow 11 \,|\, \sum_{i=0}^{k} (-1)^i \cdot a_i.$$

■

Příklad 4.10
Určete, zda číslo 242 je dělitelné číslem 11.

$242 = 2 \cdot 10^2 + 4 \cdot 10^1 + 2.$

Z důkazu Tvrzení 4.11 plyne, že

$$\begin{aligned} 11|n \quad &\Leftrightarrow \quad 11 \,|\, \sum_{i=0}^{k} (-1)^i \cdot a_i \\ 11|242 \quad &\Leftrightarrow \quad 11 \,|\, (-1)^0 \cdot 2 + (-1)^1 \cdot 4 + (-1)^2 \cdot 2 \\ &\Leftrightarrow \quad 11 \,|\, 2 - 4 + 2 \\ &\Leftrightarrow \quad 11 \,|\, 0 \end{aligned}$$

Číslo 11 *dělí* číslo 0 a to znamená, že číslo 242 je dělitelné jedenácti.

4.1.11 Dělitelnost dvanácti

Tvrzení 4.12 *Číslo $n \in \mathbb{N}$ je dělitelné dvanácti právě tehdy, když*

$$12 \mid n \Leftrightarrow \left(3 | \sum_{i=0}^{k} a_i \ \wedge \ 4 | (a_1 + a_0) \right).$$

Důkaz. Podle Tvrzení 4.2 a Tvrzení 4.3 nastane, že

$$12 \mid n \Leftrightarrow (3|n \ \wedge \ 4|n).$$

■

Tvrzení 4.13 *Číslo $n \in \mathbb{N}$ je dělitelné dvanácti právě tehdy, když*

$$12 \mid n \Leftrightarrow 12 \mid \left(4 \cdot \sum_{i=2}^{k} a_i + 10a_1 + a_0 \right).$$

Důkaz. Nechť n je přirozené číslo a $a_k a_{k-1} \ldots a_0$ je jeho ciferný zápis, tzn.

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0.$$

Uvažme, že

$$\begin{aligned} 10^1 &\equiv 10 \,(\mathrm{mod} 12) \\ 10^2 &\equiv 4 \,(\mathrm{mod} 12) \\ 10^3 &\equiv 4 \,(\mathrm{mod} 12) \\ 10^4 &\equiv 4 \,(\mathrm{mod} 12) \\ &\vdots \end{aligned}$$

Indukcí je možné snadno dokázat, že

$$\forall k \in \mathbb{N}, k \geq 2 : \quad 10^k \equiv 4 \,(\mathrm{mod} 12).$$

Proto

$$\begin{aligned} 12 \mid n \quad &\Leftrightarrow \quad n \equiv 0 \,(\mathrm{mod} 12) \\ &\Leftrightarrow \quad a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv 0 \,(\mathrm{mod} 12) \\ &\Leftrightarrow \quad a_k \cdot 4 + a_{k-1} \cdot 4 + \ldots + a_2 \cdot 4 + a_1 \cdot 10 + a_0 \equiv 0 \,(\mathrm{mod} 12) \qquad (12) \\ &\Leftrightarrow \quad 12 \mid 4 \cdot \sum_{i=2}^{k} a_i + a_1 \cdot 10 + a_0 \equiv 0 \,(\mathrm{mod} 12) \end{aligned}$$

Z (12) plyne, že

$$12 \mid n \Leftrightarrow 12 \mid \left(4 \cdot \sum_{i=2}^{k} a_i + 10a_1 + a_0 \right).$$

■

Příklad 4.11
Určete, zda číslo 144 je dělitelné číslem 12.

$144 = 1 \cdot 10^2 + 4 \cdot 10^1 + 4.$

Z důkazu Tvrzení 4.13 plyne, že

$$\begin{aligned} 12|n &\Leftrightarrow 12 \,|\, 4 \cdot \sum_{i=2}^{k} a_i + a_1 \cdot 10 + a_0 \\ 12|144 &\Leftrightarrow 12 \,|\, 1 \cdot 4 + 4 \cdot 10 + 4 \\ &\Leftrightarrow 12 \,|\, 48 \end{aligned}$$

Číslo 12 *dělí* číslo 48 a to znamená, že číslo 144 je dělitelné dvanácti.

4.1.12 Dělitelnost prvočíslem

Tvrzení 4.14 *Číslo $n \in \mathbb{N}$ je dělitelné prvočíslem p, $p \notin \{2, 5\}$ právě tehdy, když platí*

$$\sum_{j=0}^{p-1} b_j \cdot \sum_{i=0}^{q-1} (a_{i(p-1)+j}) + (a_{q(p-1)} \cdot 1 + a_{q(p-1)+1} \cdot b_1 + \ldots + a_{q(p-1)+r} \cdot b_r) \equiv 0 \,(\mathrm{mod} p),$$

kde $b_j \in \{0, 1, 2, \ldots, p-1\}$, $b_j \equiv 10^j \,(\mathrm{mod}\, p)$, $k+1 = q \cdot (p-1) + r$, kde $0 \leq r < p-1, q \in \mathbb{Z}$.

Důkaz. Pro každé prvočíslo $p \neq \{2, 5\}:\ 10^{p-1} \equiv 1 \,(\mathrm{mod} p)$. Nechť n je přirozené číslo a platí

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 \equiv 0 \,(\mathrm{mod} p).$$

Jistě existují čísla $b_1, b_2, \ldots, b_p \in \{0, 1, \ldots, p-1\}$ splňující

$$\begin{aligned} 10^0 &\equiv b_0 \,(\mathrm{mod} p) \\ 10^1 &\equiv b_1 \,(\mathrm{mod} p) \\ 10^2 &\equiv b_2 \equiv b_1^2 \,(\mathrm{mod} p) \\ 10^3 &\equiv b_3 \equiv b_1^3 \,(\mathrm{mod} p) \\ &\vdots \\ 10^{p-2} &\equiv b_{p-2} \equiv b_1^{p-2} \,(\mathrm{mod} p) \\ 10^{p-1} &\equiv b_0 \,(\mathrm{mod} p) \\ 10^p &\equiv b_1 \,(\mathrm{mod} p) \\ 10^{p+1} &\equiv b_2 \,(\mathrm{mod} p) \\ &\vdots \end{aligned}$$

Výše uvedené kongruence plynou z malé Fermatovy věty. Jestliže $k+1 = q \cdot (p-1) + r$, kde $0 \leq r < p-1, q \in \mathbb{Z}$, pak platí

$$\begin{gathered} a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 \equiv \\ (a_0 \cdot 1 + a_1 \cdot b_1 + \ldots + a_{p-2} \cdot b_{p-2}) + \\ + (a_{p-1} \cdot 1 + a_p \cdot b_1 + \ldots + a_{2p-3} \cdot b_{p-2}) + \end{gathered}$$

$$+(a_{2(p-1)} \cdot 1 + a_{2(p-1)+1} \cdot b_1 + \ldots + a_{2(p-1)+p-2} \cdot b_{p-2}) +$$
$$\vdots$$
$$+(a_{q(p-1)} \cdot 1 + a_{q(p-1)+1} \cdot b_1 + \ldots + a_{q(p-1)+r} \cdot b_r) =$$
$$= b_0 \cdot \sum_{i=0}^{q-1}(a_{i(p-1)}) + b_1 \cdot \sum_{i=0}^{q-1}(a_{i(p-1)+1}) +$$
$$\vdots$$
$$+b_{p-2} \cdot \sum_{i=0}^{q-1}(a_{i(p-1)+p-2}) + (a_{q(p-1)} \cdot 1 + a_{q(p-1)+1} \cdot b_1 + \ldots + a_{q(p-1)+r} \cdot b_r) \equiv 0 \ (\mathrm{mod} p).$$

Předchozí rovnost lze také napsat ve zkráceném tvaru

$$\sum_{j=0}^{p-b} b_j \cdot \sum_{i=0}^{q-1}(a_{i(p-1)+j}) + (a_{q(p-1)} \cdot 1 + a_{q(p-1)+1} \cdot b_1 + \ldots + a_{q(p-1)+r} \cdot b_r) \equiv 0 \ (\mathrm{mod} p).$$

■

4.2 Rychlý přehled kritérií v desítkové soustavě

n	Kritérium dělitelnosti
2	$2\|n \Leftrightarrow 2\|a_0$
3	$3\|n \Leftrightarrow 3\|\sum_{i=0}^{k} a_i$
4	$4\|n \Leftrightarrow 4\|2a_1 + a_0$
5	$5\|n \Leftrightarrow 5\|a_0$
6	$6\|n \Leftrightarrow 6\|(2\|n \ \wedge \ 3\|n)$ $6\|n \Leftrightarrow 6\|4 \cdot \sum_{i=1}^{k} a_i + a_0$
7	$7\|n \Leftrightarrow 7\|1 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 6+0}) + 3 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 6+1}) + 2 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 6+2}) + 6 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 6+3}) +$ $+4 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 6+4}) + 5 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 6+5}) + a_{q6} \cdot 1 + a_{q6+1} \cdot 3 + \ldots + a_{q6+r} \cdot b_r$
8	$8\|n \Leftrightarrow 8\|4a_2 + 2a_1 + a_0$
9	$9\|n \Leftrightarrow 9\|\sum_{i=0}^{k} a_i$
10	$10\|n \Leftrightarrow 10\|a_0$
11	$11\|n \Leftrightarrow 11\|\sum_{i=0}^{k}(-1)^i \cdot a_i$
12	$12\|n \Leftrightarrow 12\|(3\|n \ \wedge \ 4\|n)$ $12\|n \Leftrightarrow 12\|\left(4 \cdot \sum_{i=2}^{k} a_i + 10a_1 + a_0\right)$

4.3 Kritéria v binární soustavě

V této části 4. kapitoly budeme zkoumat dělitelnost čísla $n \in \mathbb{N}$, jehož ciferný zápis v binární soustavě je $a_k a_{k-1} \dots a_0$. To znamená, že

$$n = a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \ldots + a_2 \cdot 2^2 + a_1 \cdot 2 + a_0,$$

kde $\forall i \in \{k, k-1, \dots, 0\} : a_i \in \{0, 1\}$.

4.3.1 Dělitelnost dvěma

Tvrzení 4.15 *Číslo $n \in \mathbb{N}$ je dělitelné dvěma právě tehdy, když poslední cifra čísla n je 0.*

Důkaz. Nechť $n \in \mathbb{N}$ a $a_k a_{k-1} \dots a_0$ je jeho ciferný zápis, tzn.

$$n = a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \ldots + a_1 \cdot 2 + a_0.$$

Uvažme, že

$$\begin{aligned} 2^0 &\equiv 1 \,(\mathrm{mod} 2) \\ 2^1 &\equiv 0 \,(\mathrm{mod} 2) \\ 2^2 &\equiv 0 \,(\mathrm{mod} 2) \\ 2^3 &\equiv 0 \,(\mathrm{mod} 2) \\ &\vdots \end{aligned}$$

Indukcí je možné snadno dokázat, že

$$\forall k \in \mathbb{N} : \quad 2^k \equiv 0 \,(\mathrm{mod} 2).$$

Číslo n je dělitelné dvěma právě tehdy, když

$$\begin{aligned} 2 \,|\, n \quad &\Leftrightarrow \quad n \equiv 0 \,(\mathrm{mod} 2) \\ &\Leftrightarrow \quad a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \ldots + a_1 \cdot 2 + a_0 \equiv 0 \,(\mathrm{mod} 2) \\ &\Leftrightarrow \quad a_k \cdot 0 + a_{k-1} \cdot 0 + \cdots + a_1 \cdot 0 + a_0 \equiv 0 \,(\mathrm{mod} 2) \\ &\Leftrightarrow \quad a_0 \equiv 0 \,(\mathrm{mod} 2) \end{aligned} \tag{13}$$

Z (13) tak plyne, že

$$2 \,|\, n \Leftrightarrow 2 | a_0, \quad a_0 = 0.$$

■

Příklad 4.12
Určete, zda číslo $(1010)_2$ je dělitelné číslem 2.

$(1010)_2 = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0.$

Z důkazu Tvrzení 4.15 plyne, že

$$\begin{aligned} 2 | n \quad &\Leftrightarrow \quad 2 \,|\, a_0 \\ 2 | (1010)_2 \quad &\Leftrightarrow \quad 2 \,|\, 0 \end{aligned}$$

Číslo 2 *dělí* číslo 0 a to znamená, že číslo $(1010)_2$ je dělitelné dvěma.

4.3.2 Dělitelnost třemi

Tvrzení 4.16 *Číslo $n \in \mathbb{N}$ je dělitelné třemi právě tehdy, když rozdíl součtu číslic na sudém a lichém místě je dělitelný 3.*

Důkaz. Nechť $n \in \mathbb{N}$ a $a_k a_{k-1} \dots a_0$ je jeho ciferný zápis, tzn.

$$n = a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \ldots + a_1 \cdot 2 + a_0.$$

Uvažme, že

$$\begin{aligned} 2^1 &\equiv -1\,(\mathrm{mod}3) \\ 2^2 &\equiv 1\,(\mathrm{mod}3) \\ 2^3 &\equiv -1\,(\mathrm{mod}3) \\ 2^4 &\equiv 1\,(\mathrm{mod}3) \\ &\vdots \\ 2^k &\equiv (-1)^k\,(\mathrm{mod}3) \end{aligned}$$

Číslo n je dělitelné třemi právě tehdy, když

$$\begin{aligned} 3 \,|\, n &\Leftrightarrow n \equiv 0\,(\mathrm{mod}3) \\ &\Leftrightarrow a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \ldots + a_1 \cdot 2 + a_0 \equiv 0\,(\mathrm{mod}3) \\ &\Leftrightarrow a_k \cdot (-1)^k + a_{k-1} \cdot (-1)^{k-1} + \ldots + a_1 \cdot (-1) + a_0 \equiv 0\,(\mathrm{mod}3) \\ &\Leftrightarrow a_k \cdot (-1)^k + \cdots + a_4 - a_3 + a_2 - a_1 + a_0 \equiv 0\,(\mathrm{mod}3) \\ &\Leftrightarrow \sum_{i=0}^{k} (-1)^i \cdot a_i \equiv 0\,(\mathrm{mod}3) \end{aligned} \tag{14}$$

Z (14) tak plyne, že

$$3 \,|\, n \Leftrightarrow 3| \sum_{i=0}^{k} (-1)^i \cdot a_i.$$

■

Příklad 4.13
Určete, zda číslo $(1100)_2$ je dělitelné číslem 3.

$(1100)_2 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0.$

Z důkazu Tvrzení 4.16 plyne, že

$$\begin{aligned} 3|n &\Leftrightarrow 3 \,|\, \sum_{i=0}^{k} (-1)^i \cdot a_i \\ 3|(1100)_2 &\Leftrightarrow 3 \,|\, -1 + 1 - 0 + 0 \\ &\Leftrightarrow 3 \,|\, 0 \end{aligned}$$

Číslo 3 *dělí* číslo 0 a to znamená, že číslo $(1100)_2$ je dělitelné třemi.

4.3.3 Dělitelnost čtyřmi

Tvrzení 4.17 *Číslo $n \in \mathbb{N}$ je dělitelné čtyřmi právě tehdy, když součet jeho poslední cifry a dvojnásobku předposlední cifry je dělitelný číslem čtyři.*

Důkaz. Nechť $n \in \mathbb{N}$ a $a_k a_{k-1} \dots a_0$ je jeho ciferný zápis, tzn.

$$n = a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \ldots + a_1 \cdot 2 + a_0.$$

Uvažme, že

$$\begin{aligned} 2^0 &\equiv 1 \,(\mathrm{mod} 4) \\ 2^1 &\equiv 2 \,(\mathrm{mod} 4) \\ 2^2 &\equiv 0 \,(\mathrm{mod} 4) \\ 2^3 &\equiv 0 \,(\mathrm{mod} 4) \\ 2^4 &\equiv 0 \,(\mathrm{mod} 4) \\ &\vdots \end{aligned}$$

Indukcí je možné snadno dokázat, že

$$\forall k \in \mathbb{N}, k \geq 2 : \quad 2^k \equiv 0 \,(\mathrm{mod} 4).$$

Číslo n je dělitelné čtyřmi právě tehdy, když

$$\begin{aligned} 4 \,|\, n \quad &\Leftrightarrow \quad n \equiv 0 \,(\mathrm{mod} 4) \\ &\Leftrightarrow \quad a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \ldots + a_1 \cdot 2 + a_0 \equiv 0 \,(\mathrm{mod} 4) \\ &\Leftrightarrow \quad a_k \cdot 0 + a_{k-1} \cdot 0 + \ldots + a_1 \cdot 2 + a_0 \equiv 0 \,(\mathrm{mod} 4) \\ &\Leftrightarrow \quad 2a_1 + a_0 \equiv 0 \,(\mathrm{mod} 4) \end{aligned} \tag{15}$$

Z (15) tak plyne, že

$$4 \,|\, n \Leftrightarrow 4 \,|\, 2a_1 + a_0.$$

■

Příklad 4.14
Určete, zda číslo $(11100)_2$ je dělitelné číslem 4.

$(11100)_2 = 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0.$

Z důkazu Tvrzení 4.17 plyne, že

$$\begin{aligned} 4|n \quad &\Leftrightarrow \quad 4 \,|\, 2a_1 + a_0 \\ 4|(11100)_2 \quad &\Leftrightarrow \quad 4 \,|\, 2 \cdot 0 + 0 \\ &\Leftrightarrow \quad 4 \,|\, 0 \end{aligned}$$

Číslo 4 *dělí* číslo 0 a to znamená, že číslo $(11100)_2$ je dělitelné čtyřmi.

4.3.4 Dělitelnost pěti

Tvrzení 4.18 *Číslo $n \in \mathbb{N}$ je dělitelné pěti právě tehdy, když*

$$5 \,|\, n \quad \Leftrightarrow \quad 5 \,|\, \left(1 \cdot \sum_{i=0}^{q-1} (a_{i\cdot 4+0}) + 2 \cdot \sum_{i=0}^{q-1} (a_{i\cdot 4+1}) - 1 \cdot \sum_{i=0}^{q-1} (a_{i\cdot 4+2}) - 2 \cdot \sum_{i=0}^{q-1} (a_{i\cdot 4+3}) + \sum_{i=0}^{r} b_i \cdot a_{q\cdot k+i} \right),$$

kde $b_0 = 1, b_1 = 2, b_2 = -1, b_3 = -2$ a $k = q \cdot 4 + r$, kde $0 \leq r < 4$, $q \in \mathbb{Z}$.

Důkaz. Nechť $n \in \mathbb{N}$ a $a_k a_{k-1} \ldots a_0$ je jeho ciferný zápis, tzn.

$$n = a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \ldots + a_1 \cdot 2 + a_0.$$

Uvažme, že

$$\begin{aligned} 2^0 &\equiv 1 \,(\mathrm{mod} 5) \\ 2^1 &\equiv 2 \,(\mathrm{mod} 5) \\ 2^2 &\equiv -1 \,(\mathrm{mod} 5) \\ 2^3 &\equiv -2 \,(\mathrm{mod} 5) \\ 2^4 &\equiv 1 \,(\mathrm{mod} 5) \\ 2^5 &\equiv 2 \,(\mathrm{mod} 5) \\ &\vdots \end{aligned}$$

Označme $b_0 = 1, b_1 = 2, b_2 = -1, b_3 = -2$. Jestliže $k = q \cdot 4 + r$, kde $0 \leq r < 4$, $q \in \mathbb{Z}$, pak z Věty 3.4 (malá Fermatova věta) plyne, že

$$5 \,|\, n \quad \Leftrightarrow \quad 5 \,|\, \left(1 \cdot \sum_{i=0}^{q-1} (a_{i\cdot 4+0}) + 2 \cdot \sum_{i=0}^{q-1} (a_{i\cdot 4+1}) - 1 \cdot \sum_{i=0}^{q-1} (a_{i\cdot 4+2}) - 2 \cdot \sum_{i=0}^{q-1} (a_{i\cdot 4+3}) + \sum_{i=0}^{r} b_i \cdot a_{q\cdot 4+i} \right).$$

■

Příklad 4.15
Určete, zda číslo $(10100)_2$ je dělitelné číslem 5.

$(10100)_2 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0.$

Z důkazu Tvrzení 4.18 plyne, že

$$\begin{aligned} 5|(10100)_2 &\Leftrightarrow 5 \,|\, 1 \cdot 0 + 0 \cdot 2 - 1 \cdot 1 - 2 \cdot 0 + 1 \cdot 1 \\ &\Leftrightarrow 5 \,|\, 0 + 0 - 1 - 0 + 1 \\ &\Leftrightarrow 5 \,|\, 0 \end{aligned}$$

Číslo 5 *dělí* číslo 0 a to znamená, že číslo $(10100)_2$ je dělitelné pěti.

4.3.5 Dělitelnost šesti

Tvrzení 4.19 *Číslo $n \in \mathbb{N}$ je dělitelné šesti právě tehdy, když*

$$6 \mid n \Leftrightarrow 6 \mid 4 \cdot \sum_{i=1}^{k} (-1)^i \cdot a_i + a_0.$$

Důkaz. Nechť $n \in \mathbb{N}$ a $a_k a_{k-1} \ldots a_0$ je jeho ciferný zápis, tzn.

$$n = a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \ldots + a_1 \cdot 2 + a_0.$$

Uvažme, že

$$\begin{aligned} 2^0 &\equiv 1 \,(\mathrm{mod} 6) \\ 2^1 &\equiv -4 \,(\mathrm{mod} 6) \\ 2^2 &\equiv 4 \,(\mathrm{mod} 6) \\ 2^3 &\equiv -4 \,(\mathrm{mod} 6) \\ 2^4 &\equiv 4 \,(\mathrm{mod} 6) \\ &\vdots \end{aligned}$$

Indukcí je možné snadno dokázat, že

$$\forall k \in \mathbb{N}: \quad 2^k \equiv 4 \cdot (-1)^k \,(\mathrm{mod} 6).$$

Číslo n je dělitelné šesti právě tehdy, když

$$\begin{aligned} 6 \mid n \quad &\Leftrightarrow \quad n \equiv 0 \,(\mathrm{mod} 6) \\ &\Leftrightarrow \quad a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \ldots + a_1 \cdot 2 + a_0 \equiv 0 \,(\mathrm{mod} 6) \\ &\Leftrightarrow \quad a_k \cdot 4 \cdot (-1)^k + a_{k-1} \cdot 4 \cdot (-1)^{k-1} + \ldots + a_1 \cdot 4 \cdot (-1) + a_0 \equiv 0 \,(\mathrm{mod} 6) \\ &\Leftrightarrow \quad a_k \cdot 4 \cdot (-1)^k + \ldots + 4a_4 - 4a_3 + 4a_2 - 4a_1 + a_0 \equiv 0 \,(\mathrm{mod} 6) \end{aligned} \tag{16}$$

Z (16) tak plyne, že

$$6 \mid n \Leftrightarrow 6 \mid 4 \cdot \sum_{i=1}^{k} (-1)^i \cdot a_i + a_0.$$

■

Příklad 4.16
Určete, zda číslo $(10010)_2$ je dělitelné číslem 6.

$(10010)_2 = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0.$

Z důkazu Tvrzení 4.19 plyne, že

$$\begin{aligned} 6|n \quad &\Leftrightarrow \quad 6 \mid 4 \cdot \sum_{i=1}^{k} (-1)^i \cdot a_i + a_0 \\ 6|(10010)_2 \quad &\Leftrightarrow \quad 6 \mid 4 \cdot (-1 + 0 - 0 + 1) + 0 \\ &\Leftrightarrow \quad 6 \mid 0 \end{aligned}$$

Číslo 6 *dělí* číslo 0 a to znamená, že číslo $(10010)_2$ je dělitelné šesti.

4.3.6 Dělitelnost sedmi

Tvrzení 4.20 *Číslo $n \in \mathbb{N}$ je dělitelné sedmi právě tehdy, když*

$$7 \,|\, n \quad \Leftrightarrow \quad 7 \,|\, \left(1 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 3+0}) + 2 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 3+1}) + 4 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 3+2}) + \sum_{i=0}^{r} b_i \cdot a_{q\cdot 3+i}\right),$$

kde $b_0 = 1, b_1 = 2, b_2 = 4$ a $k+1 = q \cdot 3 + r$, kde $0 \leq r < 3$, $q \in \mathbb{Z}$.

Důkaz. Nechť $n \in \mathbb{N}$ a $a_k a_{k-1} \ldots a_0$ je jeho ciferný zápis, tzn.

$$n = a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \ldots + a_1 \cdot 2 + a_0.$$

Uvažme, že

$$\begin{aligned} 2^0 &\equiv 1\,(\mathrm{mod}7) \\ 2^1 &\equiv 2\,(\mathrm{mod}7) \\ 2^2 &\equiv 4\,(\mathrm{mod}7) \\ 2^3 &\equiv 1\,(\mathrm{mod}7) \\ 2^4 &\equiv 2\,(\mathrm{mod}7) \\ 2^5 &\equiv 4\,(\mathrm{mod}7) \\ &\vdots \end{aligned}$$

Označme $b_0 = 1, b_1 = 2, b_2 = 4$. Jestliže $k+1 = q \cdot 3 + r$, kde $0 \leq r < 3$, $q \in \mathbb{Z}$, pak z Věty 3.4 (malá Fermatova věta) plyne, že

$$7 \,|\, n \quad \Leftrightarrow \quad 7 \,|\, \left(1 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 3+0}) + 2 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 3+1}) + 4 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 3+2}) + \sum_{i=0}^{r} b_i \cdot a_{q\cdot 3+i}\right).$$

■

Příklad 4.17
Určete, zda číslo $(100011)_2$ je dělitelné číslem 7.

$(100011)_2 = 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1.$

Z důkazu Tvrzení 4.20 plyne, že

$$\begin{aligned} 7|(100011)_2 &\Leftrightarrow 7 \,|\, 1 \cdot 4 + 0 \cdot 2 + 0 \cdot 1 + 0 \cdot 4 + 1 \cdot 2 + 1 \cdot 1 \\ &\Leftrightarrow 7 \,|\, 4 + 0 + 0 + 0 + 2 + 1 \\ &\Leftrightarrow 7 \,|\, 7 \end{aligned}$$

Číslo 7 *dělí* číslo 7 a to znamená, že číslo $(100011)_2$ je dělitelné sedmi.

4.3.7 Dělitelnost osmi

Tvrzení 4.21 *Číslo $n \in \mathbb{N}$ je dělitelné osmi právě tehdy, když*

$$8 \,|\, n \Leftrightarrow 8 \,|\, 4a_2 + 2a_1 + a_0.$$

Důkaz. Nechť $n \in \mathbb{N}$ a $a_k a_{k-1} \ldots a_0$ je jeho ciferný zápis, tzn.

$$n = a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \ldots + a_1 \cdot 2 + a_0.$$

Uvažme, že

$$\begin{aligned} 2^0 &\equiv 1\,(\mathrm{mod}8) \\ 2^1 &\equiv 2\,(\mathrm{mod}8) \\ 2^2 &\equiv 4\,(\mathrm{mod}8) \\ 2^3 &\equiv 0\,(\mathrm{mod}8) \\ 2^4 &\equiv 0\,(\mathrm{mod}8) \\ &\vdots \end{aligned}$$

Indukcí je možné snadno dokázat, že

$$\forall k \in \mathbb{N}, k \geq 3: \quad 2^k \equiv 0\,(\mathrm{mod}8).$$

Číslo n je dělitelné osmi právě tehdy, když

$$\begin{aligned} 8 \,|\, n &\Leftrightarrow n \equiv 0\,(\mathrm{mod}8) \\ &\Leftrightarrow a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \ldots + a_1 \cdot 2 + a_0 \equiv 0\,(\mathrm{mod}8) \\ &\Leftrightarrow a_k \cdot 0 + a_{k-1} \cdot 0 + \ldots + a_2 \cdot 4 + a_1 \cdot 2 + a_0 \equiv 0\,(\mathrm{mod}8) \\ &\Leftrightarrow 4a_2 + 2a_1 + a_0 \equiv 0\,(\mathrm{mod}8) \end{aligned} \tag{17}$$

Z (17) tak plyne, že

$$8 \,|\, n \Leftrightarrow 8 \,|\, 4a_2 + 2a_1 + a_0.$$

■

Příklad 4.18
Určete, zda číslo $(11100)_2$ je dělitelné číslem 8.

$(11000)_2 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0.$

Z důkazu Tvrzení 4.21 plyne, že

$$\begin{aligned} 8|n &\Leftrightarrow 8 \,|\, 4a_2 + 2a_1 + a_0 \\ 8|(11000)_2 &\Leftrightarrow 8 \,|\, 4 \cdot 0 + 2 \cdot 0 + 0 \\ &\Leftrightarrow 8 \,|\, 0 \end{aligned}$$

Číslo 8 *dělí* číslo 0 a to znamená, že číslo $(11000)_2$ je dělitelné osmi.

4.3.8 Dělitelnost devíti

Tvrzení 4.22 *Číslo $n \in \mathbb{N}$ je dělitelné devíti právě tehdy, když*

$$9 \mid n \quad \Leftrightarrow \quad 9 \mid (1 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 6+0}) + 2 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 6+1}) + 4 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 6+2}) - 1 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 6+3}) - \\ - 2 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 6+4}) - 4 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 6+5}) + \sum_{i=0}^{r} b_i \cdot a_{q\cdot 6+i}),$$

kde $b_0 = 1, b_1 = 2, b_2 = 4, b_3 = -1, b_4 = -2, b_5 = -4$ a $k+1 = q \cdot 6 + r$, kde $0 \leq r < 6$, $q \in \mathbb{Z}$.

Důkaz. Nechť $n \in \mathbb{N}$ a $a_k a_{k-1} \ldots a_0$ je jeho ciferný zápis, tzn.

$$n = a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \ldots + a_1 \cdot 2 + a_0.$$

Uvažme, že

$$\begin{aligned} 2^0 &\equiv 1 \,(\mathrm{mod} 9) \\ 2^1 &\equiv 2 \,(\mathrm{mod} 9) \\ 2^2 &\equiv 4 \,(\mathrm{mod} 9) \\ 2^3 &\equiv -1 \,(\mathrm{mod} 9) \\ 2^4 &\equiv -2 \,(\mathrm{mod} 9) \\ 2^5 &\equiv -4 \,(\mathrm{mod} 9) \\ 2^6 &\equiv 1 \,(\mathrm{mod} 9) \\ &\vdots \end{aligned}$$

Označme $b_0 = 1, b_1 = 2, b_2 = 4, b_3 = -1, b_4 = -2, b_5 = -4$. Jestliže $k+1 = q \cdot 6 + r$, kde $0 \leq r < 6$, $q \in \mathbb{Z}$, tak dostaneme

$$9 \mid n \quad \Leftrightarrow \quad 9 \mid (1 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 6+0}) + 2 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 6+1}) + 4 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 6+2}) - 1 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 6+3}) - \\ - 2 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 6+4}) - 4 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 6+5}) + \sum_{i=0}^{r} b_i \cdot a_{q\cdot 6+i}).$$

■

Příklad 4.19
Určete, zda číslo $(101101)_2$ je dělitelné číslem 9.

$(101101)_2 = 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1.$

Z důkazu Tvrzení 4.22 plyne, že

$$\begin{aligned} 9|(101101)_2 &\Leftrightarrow 9 \mid 1 \cdot (-4) + 0 \cdot (-2) + 1 \cdot (-1) + 1 \cdot 4 + 0 \cdot 2 + 1 \cdot 1 \\ &\Leftrightarrow 9 \mid -4 + 0 - 1 + 4 + 0 + 1 \\ &\Leftrightarrow 9 \mid 0 \end{aligned}$$

Číslo 9 *dělí* číslo 0 a to znamená, že číslo $(101101)_2$ je dělitelné devíti.

4.3.9 Dělitelnost deseti

Tvrzení 4.23 *Číslo $n \in \mathbb{N}$ je dělitelné deseti právě tehdy, když*

$$10 \,|\, n \quad \Leftrightarrow \quad 10 \,|\, (a_0 + 2 \cdot \sum_{i=0}^{q-1} (a_{i\cdot 4+1}) + 4 \cdot \sum_{i=0}^{q-1} (a_{i\cdot 4+2}) - 2 \cdot \sum_{i=0}^{q-1} (a_{i\cdot 4+3}) - \\ - 4 \cdot \sum_{i=0}^{q-1} (a_{i\cdot 4+4}) + \sum_{i=0}^{r} b_i \cdot a_{q\cdot 4+i}),$$

kde $b_1 = 2, b_2 = 4, b_3 = -2, b_4 = -4$ a $k = q \cdot 4 + r$, kde $0 \leq r < 4$, $q \in \mathbb{Z}$.

Důkaz. Nechť $n \in \mathbb{N}$ a $a_k a_{k-1} \ldots a_0$ je jeho ciferný zápis, tzn.

$$n = a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \ldots + a_1 \cdot 2 + a_0.$$

Uvažme, že

$$\begin{aligned} 2^0 &\equiv 1 \,(\mathrm{mod} 10) \\ 2^1 &\equiv 2 \,(\mathrm{mod} 10) \\ 2^2 &\equiv 4 \,(\mathrm{mod} 10) \\ 2^3 &\equiv -2 \,(\mathrm{mod} 10) \\ 2^4 &\equiv -4 \,(\mathrm{mod} 10) \\ 2^5 &\equiv 2 \,(\mathrm{mod} 10) \\ 2^6 &\equiv 4 \,(\mathrm{mod} 10) \\ &\vdots \end{aligned}$$

Označme $b_1 = 2, b_2 = 4, b_3 = -2, b_4 = -4$. Jestliže $k = q \cdot 4 + r$, kde $0 \leq r < 4$, $q \in \mathbb{Z}$, tak dostaneme

$$10 \,|\, n \quad \Leftrightarrow \quad 10 \,|\, (a_0 + 2 \cdot \sum_{i=0}^{q-1} (a_{i\cdot 4+1}) + 4 \cdot \sum_{i=0}^{q-1} (a_{i\cdot 4+2}) - 2 \cdot \sum_{i=0}^{q-1} (a_{i\cdot 4+3}) - \\ - 4 \cdot \sum_{i=0}^{q-1} (a_{i\cdot 4+4}) + \sum_{i=0}^{r} b_i \cdot a_{q\cdot 4+i}).$$

■

Příklad 4.20
Určete, zda číslo $(110010)_2$ je dělitelné číslem 10.

$(110010)_2 = 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0.$

Z důkazu Tvrzení 4.23 plyne, že

$$\begin{aligned} 10|(110010)_2 &\Leftrightarrow 10 \,|\, 0 + 1 \cdot 2 + 0 \cdot 4 + 0 \cdot (-2) + 1 \cdot (-4) + 1 \cdot 2 \\ &\Leftrightarrow 10 \,|\, 0 + 2 + 0 - 0 - 4 + 2 \\ &\Leftrightarrow 10 \,|\, 0 \end{aligned}$$

Číslo 10 *dělí* číslo 0 a to znamená, že číslo $(110010)_2$ je dělitelné deseti.

4.3.10 Dělitelnost jedenácti

Tvrzení 4.24 *Číslo $n \in \mathbb{N}$ je dělitelné jedenácti právě tehdy, když*

$$\begin{aligned} 11 \mid n \quad \Leftrightarrow \quad & 11 \mid (1 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 10+0}) + 2 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 10+1}) + 4 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 10+2}) - 3 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 10+3}) + \\ & + 5 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 10+4}) - 1 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 10+5}) - 2 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 10+6}) - 4 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 10+7}) + \\ & + 3 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 10+8}) - 5 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 10+9}) + \sum_{i=0}^{r} b_i \cdot a_{q\cdot 10+i}), \end{aligned}$$

kde $b_0 = 1, b_1 = 2, b_2 = 4, b_3 = -3, b_4 = 5, b_5 = -1, b_6 = -2, b_7 = -4, b_8 = 3, b_9 = -5$ a $k + 1 = q \cdot 10 + r$, kde $0 \leq r < 10$, $q \in \mathbb{Z}$.

Důkaz. Nechť $n \in \mathbb{N}$ a $a_k a_{k-1} \ldots a_0$ je jeho ciferný zápis, tzn.

$$n = a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \ldots + a_1 \cdot 2 + a_0.$$

Uvažme, že

$$\begin{aligned} 2^0 &\equiv 1 \,(\mathrm{mod} 11) \\ 2^1 &\equiv 2 \,(\mathrm{mod} 11) \\ 2^2 &\equiv 4 \,(\mathrm{mod} 11) \\ 2^3 &\equiv -3 \,(\mathrm{mod} 11) \\ 2^4 &\equiv 5 \,(\mathrm{mod} 11) \\ 2^5 &\equiv -1 \,(\mathrm{mod} 11) \\ 2^6 &\equiv -2 \,(\mathrm{mod} 11) \\ 2^7 &\equiv -4 \,(\mathrm{mod} 11) \\ 2^8 &\equiv 3 \,(\mathrm{mod} 11) \\ 2^9 &\equiv -5 \,(\mathrm{mod} 11) \\ 2^{10} &\equiv 1 \,(\mathrm{mod} 11) \\ &\vdots \\ 2^{15} = 2^{5+10} &\equiv -1 \,(\mathrm{mod} 11) \\ 2^{16} = 2^{6+10} &\equiv -2 \,(\mathrm{mod} 11) \\ 2^{17} = 2^{7+10} &\equiv -4 \,(\mathrm{mod} 11) \\ &\vdots \end{aligned}$$

Označme $b_0 = 1, b_1 = 2, b_2 = 4, b_3 = -3, b_4 = 5, b_5 = -1, b_6 = -2, b_7 = -4, b_8 = 3,$ $b_9 = -5$. Jestliže $k + 1 = q \cdot 10 + r$, kde $0 \leq r < 10$, $q \in \mathbb{Z}$, pak z Věty 3.4 plyne, že

$$\begin{aligned} 11 \mid n \quad \Leftrightarrow \quad & 11 \mid (1 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 10+0}) + 2 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 10+1}) + 4 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 10+2}) - 3 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 10+3}) + \\ & + 5 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 10+4}) - 1 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 10+5}) - 2 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 10+6}) - 4 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 10+7}) + \\ & + 3 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 10+8}) - 5 \cdot \sum_{i=0}^{q-1}(a_{i\cdot 10+9}) + \sum_{i=0}^{r} b_i \cdot a_{q\cdot 10+i}). \end{aligned}$$

■

Příklad 4.21
Určete, zda číslo $(10110)_2$ je dělitelné číslem 11.

$(10110)_2 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0.$

Z důkazu Tvrzení 4.24 plyne, že

$$\begin{aligned} 11|(10110)_2 &\Leftrightarrow 11 \,|\, 1 \cdot 5 + 0 \cdot (-3) + 1 \cdot 4 + 1 \cdot 2 + 0 \cdot 1 \\ &\Leftrightarrow 11 \,|\, 5 + 4 + 2 \\ &\Leftrightarrow 11 \,|\, 11 \end{aligned}$$

Číslo 11 *dělí* číslo 11 a to znamená, že číslo $(10110)_2$ je dělitelné jedenácti.

4.3.11 Dělitelnost dvanácti

Tvrzení 4.25 *Číslo $n \in \mathbb{N}$ je dělitelné dvanácti právě tehdy, když*

$$12 \,|\, n \Leftrightarrow 12 \,|\, 4 \cdot \sum_{i=2}^{k} (-1)^i \cdot a_i + 2a_1 + a_0.$$

Důkaz. Nechť $n \in \mathbb{N}$ a $a_k a_{k-1} \ldots a_0$ je jeho ciferný zápis, tzn.

$$n = a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \ldots + a_1 \cdot 2 + a_0.$$

Uvažme, že

$$\begin{aligned} 2^0 &\equiv 1 \,(\mathrm{mod} 12) \\ 2^1 &\equiv 2 \,(\mathrm{mod} 12) \\ 2^2 &\equiv 4 \,(\mathrm{mod} 12) \\ 2^3 &\equiv -4 \,(\mathrm{mod} 12) \\ 2^4 &\equiv 4 \,(\mathrm{mod} 12) \\ 2^5 &\equiv -4 \,(\mathrm{mod} 12) \\ &\vdots \end{aligned}$$

Indukcí je možné snadno dokázat, že

$$\forall k \in \mathbb{N}, k \geq 2 : \quad 2^k \equiv 4 \cdot (-1)^k \,(\mathrm{mod} 12).$$

Číslo n je dělitelné dvanácti právě tehdy, když

$$\begin{aligned} 12 \,|\, n &\Leftrightarrow n \equiv 0 \,(\mathrm{mod} 12) \\ &\Leftrightarrow a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \ldots + a_1 \cdot 2 + a_0 \equiv 0 \,(\mathrm{mod} 12) \\ &\Leftrightarrow a_k \cdot 4 \cdot (-1)^k + \ldots + a_3 \cdot 4 \cdot (-1)^3 + a_2 \cdot 4 \cdot (-1)^2 + a_1 \cdot 2 + a_0 \equiv 0 \,(\mathrm{mod} 12) \\ &\Leftrightarrow a_k \cdot 4 \cdot (-1)^k + \ldots + 4a_4 - 4a_3 + 4a_2 + 2a_1 + a_0 \equiv 0 \,(\mathrm{mod} 12) \end{aligned} \tag{18}$$

Z (18) tak plyne, že

$$12 \,|\, n \Leftrightarrow 12 \,|\, 4 \cdot \sum_{i=2}^{k} (-1)^i \cdot a_i + 2a_1 + a_0.$$

■

Příklad 4.22
Určete, zda číslo $(11000)_2$ je dělitelné číslem 12.

$(11000)_2 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0.$

Z důkazu Tvrzení 4.22 plyne, že

$$\begin{array}{rcl} 12|n & \Leftrightarrow & 12 \,|\, 4 \cdot \sum_{i=2}^{k} (-1)^i \cdot a_i + 2a_1 + a_0 \\ 12|(11000)_2 & \Leftrightarrow & 12 \,|\, 4 \cdot (0 - 1 + 1) + 2 \cdot 0 + 0 \\ & \Leftrightarrow & 12 \,|\, 0 \end{array}$$

Číslo 12 *dělí* číslo 0 a to znamená, že číslo $(11000)_2$ je dělitelné dvanácti.

4.3.12 Dělitelnost prvočíslem

Tvrzení 4.26 *Číslo $n \in \mathbb{N}$ je dělitelné prvočíslem p, $p \neq 2$ právě tehdy, když platí*

$$\sum_{j=0}^{p-1} b_j \cdot \sum_{i=0}^{q-1} (a_{i(p-1)+j}) + (a_{q(p-1)} \cdot 1 + a_{q(p-1)+1} \cdot b_1 + \ldots + a_{q(p-1)+r} \cdot b_r) \equiv 0 \,(\mathrm{mod} p),$$

kde $b_j \in \{0, 1, 2, \ldots, p-1\}$, $b_j \equiv 2^j \,(\mathrm{mod}\, p)$ a $k+1 = q \cdot (p-1) + r$, kde $0 \leq r < p-1, q \in \mathbb{Z}$.

Důkaz. Pro každé prvočíslo $p \neq 2 :\ 2^{p-1} \equiv 1 \,(\mathrm{mod} p)$. Nechť n je přirozené číslo a platí

$$n = a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \ldots + a_1 \cdot 2 + a_0 \equiv 0 \,(\mathrm{mod} p).$$

Jistě existují čísla $b_0, b_1, b_2, \ldots, b_p \in \{0, 1, \ldots, p-1\}$ splňující

$$\begin{array}{rcl} 2^0 & \equiv & b_0 \,(\mathrm{mod} p) \\ 2^1 & \equiv & b_1 \,(\mathrm{mod} p) \\ 2^2 & \equiv & b_2 \equiv b_1^2 \,(\mathrm{mod} p) \\ 2^3 & \equiv & b_3 \equiv b_1^3 \,(\mathrm{mod} p) \\ & \vdots & \\ 2^{p-2} & \equiv & b_{p-2} \equiv b_1^{p-2} \,(\mathrm{mod} p) \\ 2^{p-1} & \equiv & b_0 \,(\mathrm{mod} p) \\ 2^p & \equiv & b_1 \,(\mathrm{mod} p) \\ 2^{p+1} & \equiv & b_2 \,(\mathrm{mod} p) \\ & \vdots & \end{array}$$

Výše uvedené kongruence plynou z malé Fermatovy věty. Jestliže $k+1 = q \cdot (p-1) + r$, kde $0 \leq r < p-1, q \in \mathbb{Z}$, pak platí

$$\begin{gathered}
a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \ldots + a_1 \cdot 2 + a_0 \equiv \\
(a_0 \cdot 1 + a_1 \cdot b_1 + \ldots + a_{p-2} \cdot b_{p-2}) + \\
+(a_{p-1} \cdot 1 + a_p \cdot b_1 + \ldots + a_{2p-3} \cdot b_{p-2}) + \\
+(a_{2(p-1)} \cdot 1 + a_{2(p-1)+1} \cdot b_1 + \ldots + a_{2(p-1)+p-2} \cdot b_{p-2}) + \\
\vdots \\
+(a_{q(p-1)} \cdot 1 + a_{q(p-1)+1} \cdot b_1 + \ldots + a_{g(p-1)+r} \cdot b_r) = \\
= b_0 \cdot \sum_{i=0}^{q-1} (a_{i(p-1)}) + b_1 \cdot \sum_{i=0}^{q-1} (a_{i(p-1)+1}) + \\
\vdots \\
+b_{p-2} \cdot \sum_{i=0}^{q-1} (a_{i(p-1)+p-2}) + (a_{q(p-1)} \cdot 1 + a_{q(p-1)+1} \cdot b_1 + \ldots + a_{q(p-1)+r} \cdot b_r) \equiv 0 \ (\mathrm{mod} p).
\end{gathered}$$

Předchozí rovnost lze také napsat ve zkráceném tvaru

$$\sum_{j=0}^{p-1} b_j \cdot \sum_{i=0}^{q-1} (a_{i(p-1)+j}) + (a_{q(p-1)} \cdot 1 + a_{q(p-1)+1} \cdot b_1 + \ldots + a_{q(p-1)+r} \cdot b_r) \equiv 0 \ (\mathrm{mod} p).$$

■

5 Testování v Matlabu

V této kapitole se budeme zabývat matematickými výpočty v programu MATLAB, kde jsou aplikována kritéria dělitelnosti obsažená v předchozích kapitolách.

Cílem bylo vytvořit program umožňující aplikovat kritéria dělitelnosti při hledání prvočísel. Fungují jako první síto, jsou numericky nenáročné a umožňují nám ve zkoumaném intervalu vyřadit "velké procento" čísel z podezření, že se jedná o prvočíslo. Jako vedlejší produkt obdržíme horní (velmi hrubý) odhad počtu prvočísel ve zkoumaném intervalu.

Musela jsem si nejprve vytvořit funkce ověřující dělitelnost daného čísla několika prvočíselnými děliteli. Pro jednoduchost jsem zvolila prvočísla 2, 3, 5, 7 a 11.

Jsou to funkce *two, three, five, seven, eleven*:

```
function [ return_value ] = two ( a )

    return_value = 0;
    x = a(end);

    if mod(x,2) == 0
        return_value = 1;
    end

end
```

Výpis 1: Dělitelnost dvěma

```
function [ return_value ] = three ( a )

    return_value = 0;
    x = sum(a);

    if mod(x,3) == 0
        return_value = 1;
    end

end
```

Výpis 2: Dělitelnost třemi

```
function [ return_value ] = five ( a )

    return_value = 0;
    x = a(end);

    if mod(x,5) == 0
        return_value = 1;
    end

end
```

Výpis 3: Dělitelnost pěti

```
function [ return_value ] = seven ( a )

    return_value = 0;
    a = convert( n );
    b = [1  3 2 6 4  5];

    vysledek = 0;
    delka = length(a);
    j = 1;
    for i = 1:delka
        if j == 7
            j = 1;
        end

    vysledek = vysledek + a(i)*b(j);
    j = j + 1;
    end

    if mod(vysledek,7) == 0
        return_value = 1;
    end

end
```

Výpis 4: Dělitelnost sedmi

```
function [ return_value ] = eleven ( a )

    return_value = 0;
    a = convert( n );

    vysledek = 0;
    delka = length(a);
    for i = 1:delka
        vysledek = vysledek + (-1)^(i) * a(i);
    end

    if mod(vysledek,11) == 0
        return_value = 1;
    end

end
```

Výpis 5: Dělitelnost jedenácti

Výstup výše uvedených funkcí je hodnota 0 nebo 1. V případě nuly to znamená, že zadané číslo n je dělitelné daným číslem se zbytkem a tudíž je možné, že číslo n je prvočíslo. V případě jedničky to znamená, že číslo n, kde $n > 11$ je dělitelné beze zbytku a stoprocentně není prvočíslem.

Zvolíme si tedy nějaké vstupní číslo n a nějaké d a spustíme výpočet pro odhad prvočísel v intervalu $\langle n, n + d\rangle$. K tomu slouží funkce *CounterPrimes*:

```
function [ ] = CounterPrimes ( n, d )

    counter = 0;
    primes = [];
    percentage = 0;

    tic () ;
    for i = n : (n + d)
        if two(i) == 0
            if three(i) == 0
                if five(i) == 0
                    if seven(i) == 0
                        if eleven(i) == 0
                            primes = [primes i];
                            counter = counter + 1;
                        end
                    end
                end
            end
        end
    end
    time = toc();

    percentage = (counter / d) * 100;

    disp(['Celkový počet podezřelých bodů: ' num2str(counter)]);
    disp(['Podezřelé body v intervalu: ' , num2str(primes)]);
    disp(['Hrubý odhad prvočísel v intervalu: ' ,num2str(percentage), ' %']);
    disp(['Čas výpočtu: ' num2str(time)]);


end
```

Výpis 6: Funkce pro výpočet odhadu prvočísel v zadaném intervalu

Výše uvedená funkce nám vypíše seznam čísel z intervalu $\langle n, n + d\rangle$, která nejsou dělitelná ani jedním z čísel 2, 3, 5, 7, 11 a jejich celkový počet. Dostáváme tak hrubý odhad počtu prvočísel v intervalu $\langle n, n + d\rangle$. Dalším výstupem je čas, jak dlouho trvalo nalézt podezřelé body z tohoto intervalu. A nakonec nám program vypíše procento hrubého odhadu prvočísel v zadaném intervalu.

Ukázka výstupu pro menší interval:

```
>> CounterPrimes(20,50)
Celkový počet podezřelých bodů: 11
Podezřelé body v intervalu: 23  29  31  37  41  43  47  53  59  61  67
Hrubý odhad prvočísel v intervalu: 22 %
Čas výpočtu: 0.0016322
```

Výpis 7: Výstup funkce *CounterPrimes*

Ukázka výstupu pro větší interval:

```
>> CounterPrimes(10000,2500)
Celkový počet podezřelých bodů: 521
Podezřelé body v intervalu: 10001 10007 10009 10013 10019 10027 10033 10037 10039 10049
    10051 10057 10061 10063 10067 10069 10079 10081 10091 10093 10097 10099 10103
    10111 10117 10121 10123 10127 10133 10139 10141 10147 10151 10159 10163 10169
    10177 10181 10183 10187 10189 10193 10201 10207 10211 10217 10223 10229 10231
    10237 10243 10247 10249 10253 10259 10261 10267 10271 10273 10277 10279 10289
    10291 10301 10303 10309 10313 10319 10321 10327 10331 10333 10337 10343 10349
    10357 10361 10363 10369 10379 10387 10391 10393 10397 10399 10403 10411 10421
    10427 10429 10433 10441 10447 10453 10457 10459 10463 10469 10471 10477 10481
    10487 10489 10499 10501 10511 10513 10517 10519 10523 10529 10531 10537 10541
    10543 10547 10553 10559 10561 10567 10573 10579 10583 10589 10597 10601 10603
    10607 10609 10613 10621 10627 10631 10639 10643 10649 10651 10657 10663 10667
    10669 10673 10679 10687 10691 10693 10697 10699 10709 10711 10721 10723 10727
    10729 10733 10739 10741 10751 10753 10757 10763 10771 10777 10781 10783 10789
    10793 10799 10807 10811 10817 10819 10823 10831 10837 10841 10847 10849 10853
    10859 10861 10867 10873 10877 10883 10889 10891 10897 10903 10907 10909 10919
    10921 10931 10933 10937 10939 10943 10949 10951 10957 10961 10963 10973 10979
    10981 10987 10991 10993 10999 11003 11009 11017 11021 11023 11027 11029 11041
    11047 11051 11057 11059 11063 11069 11071 11083 11087 11089 11093 11101  ...
Hrubý odhad prvočísel v intervalu: 20.84 %
Čas výpočtu: 0.07598
```

Výpis 8: Výstup funkce *CounterPrimes*

Z výše uvedených výsledků můžeme vidět, že tímto vytvořeným algoritmem jsme ze zadaného intervalu vyřadili přibližně 80% čísel, která nejsou prvočísla, protože jsou dělitelná alespoň jedním z čísel 2, 3, 5, 7, 11. Takže přibližně 20% čísel ze zadaného intervalu mohou být prvočísla.

Čas výpočtu není vždy stejný, záleží na

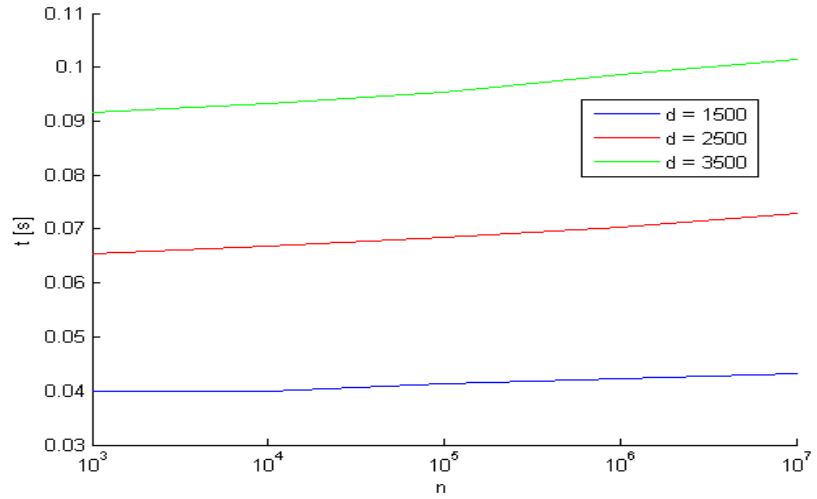
1. velikosti intervalu
2. hardware PC
3. počtu běžících procesů na pozadí počítače

Veškeré testy jsou prováděny na průměrném uživatelském počítači s dvoujádrovým procesorem Intel a pamětí 4 GB.

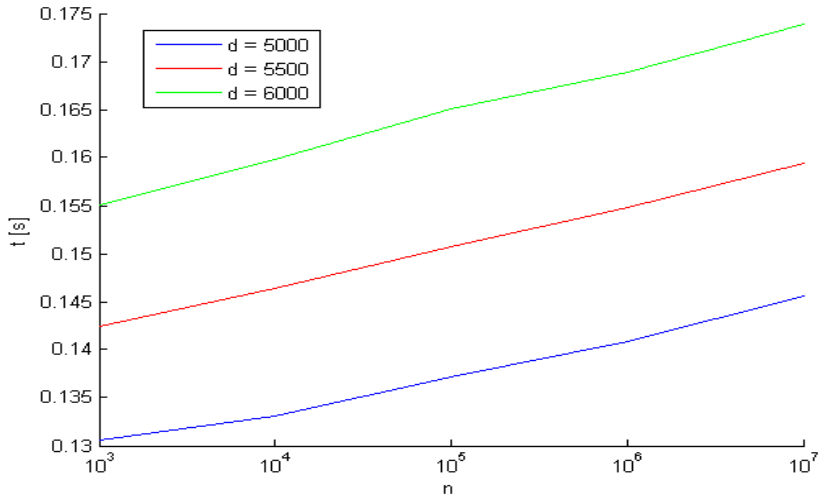
5.1 Grafy

Pro ukázku efektivnosti výpočtu poslouží pár grafů, ze kterých je vidět, jak se liší náročnost výpočtu v závislosti na čase.

Grafy s menším intervalem čísel:

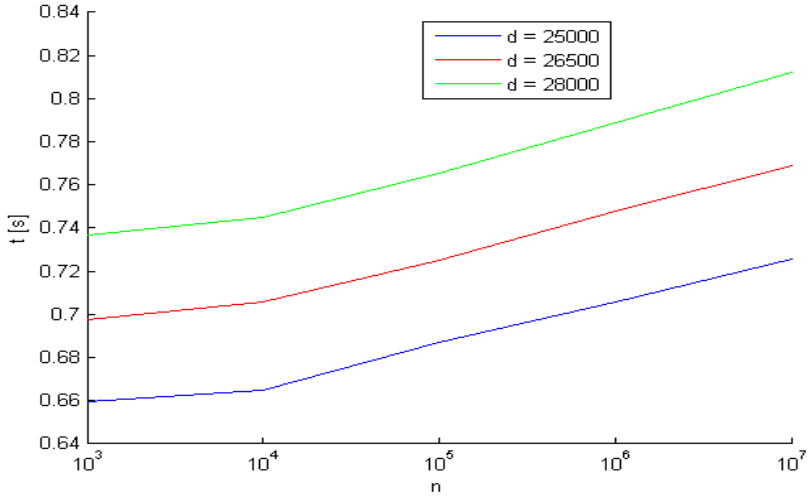


Obrázek 1: Graf č.1

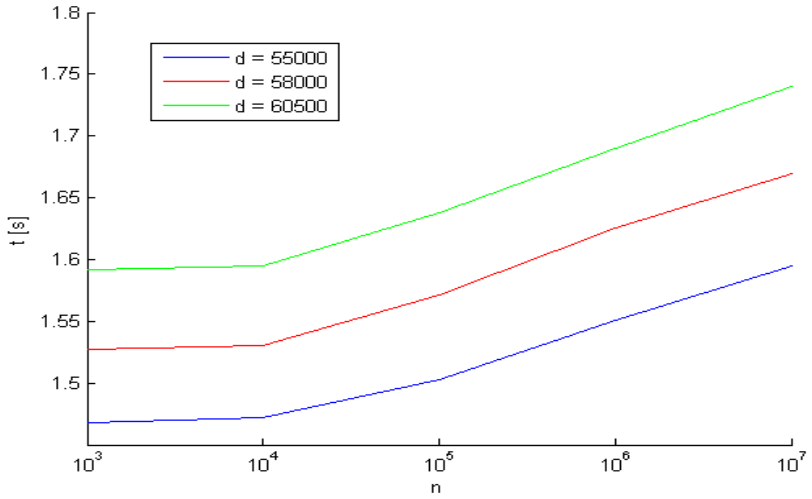


Obrázek 2: Graf č.2

Grafy s větším intervalem čísel:



Obrázek 3: Graf č.3



Obrázek 4: Graf č.4

Z výše vyobrazených grafů můžeme vidět, že časová náročnost začíná stoupat se zvětšujícím se intervalem čísel.

6 Závěr

Cílem této práce bylo vytvořit kritéria dělitelnosti, díky kterým můžeme rozhodnout, zda dané číslo zapsané ciframi určité číselné soustavy je dělitelné daným číslem. Proto je výhodné použít tato kritéria jako první síto při identifikaci prvočísel.

Odvodili jsme důkazy pro dělitelnost čísel od 2 do 12 a také obecný důkaz dělitelnosti prvočíslem. Tyto kritéria jsme odvodili pomocí kongruencí.

Jednotlivá kritéria jsme aplikovali v programu MATLAB a vytvořili software pro testování velkých čísel. Vstupem jsou dvě čísla, ze kterých vytvoříme interval. Interval procházíme vytvořenými funkcemi, ve kterých jsou aplikovány kritéria dělitelnosti z výše uvedené teorie. Odhadujeme, kolik čísel z intervalu mohou být prvočísla. Během jednotlivých výpočtu měříme čas, abychom poté mohli vytvořit závislostní graf.

Tímto testováním jsme zjistili, že záleží na mnoha faktorech, jak výpočet proběhne. Jednak to jsou hardwarové nároky počítače a také velikost zadaného intervalu čísel. Výpočty jsme prováděli na počítači s dvoujádrovým procesorem Intel s 4 GB paměti a při výpočtu intervalu o velikosti desítek miliónu čísel již tento počítač nezvládal vypočítat hrubý odhad počtu prvočísel v intervalu, takže ani odhadnout čas daného výpočtu. Bohužel nebyla možnost provádět testy na výkonnějších počítačích.

7 Literatura

[1] Pavel Jahoda: Základy teorie čísel a jejích aplikací pro nematematiky, VŠB-TU Ostrava, 2010.

[2] James Pommersheim, Tim Marks and Erica Flapan: Number Theory - A Lively Introduction with Proofs, Applications, and Stories. Wiley, 2010.

[3] Jiří Velebil: Diskrétní matematika, ČVUT Praha, 2007.